

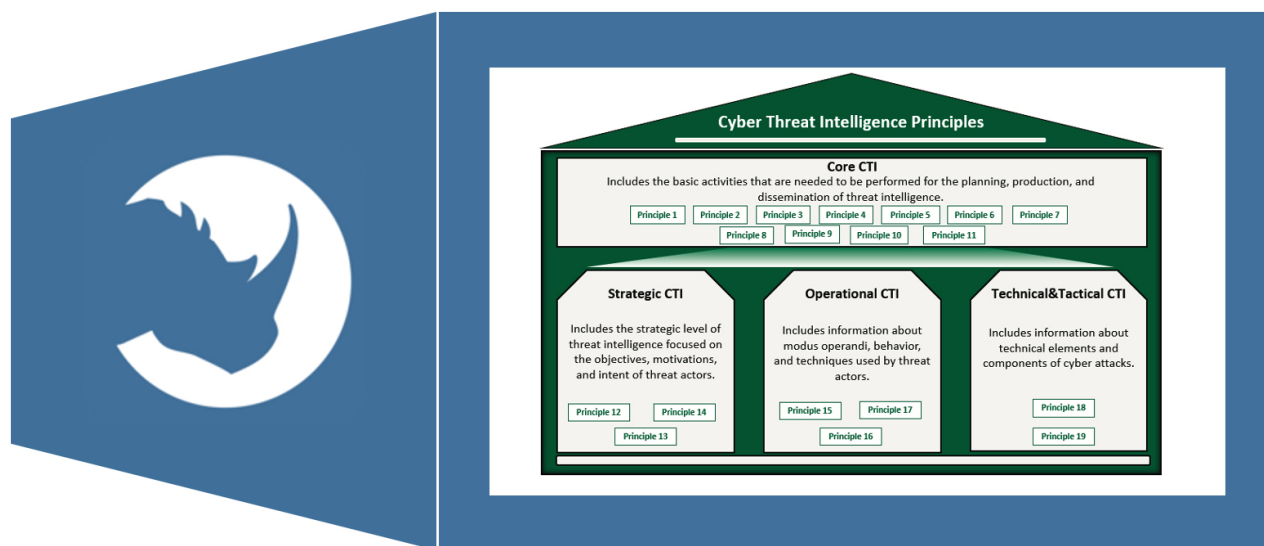
# **Role of ThreatQ in Saudi Central Bank's **Cyber Threat Intelligence Principles****

## Executive Summary

The Saudi Central Bank (SAMA) has developed Cyber Threat Intelligence (CTI) Principles framework that “describes best practices focused on producing, processing, and disseminating threat intelligence to enhance the identification and mitigation of cyber threats relevant to the financial sector in the KSA”.

As the industry's leading data-driven security operations platform for CTI and XDR, ThreatQuotient is well positioned to address the requirements defined by SAMA. This paper illustrates how ThreatQuotient directly supports each of the nineteen SAMA principles that span a range of core, strategic, operational, as well as technical & tactical domains.

ThreatQuotient directly supports SAMA principles related to data collection, aggregation and storage, and provides indirect support for those principles related to processes and roles.



## Role of ThreatQ in Cyber Threat Intelligence Principles

In the remainder of the paper, each SAMA principle is presented followed by a short description of how ThreatQuotient addresses the principle. The accompanying screenshots and images help to further illustrate how the ThreatQ platform supports SAMA's CTI framework.

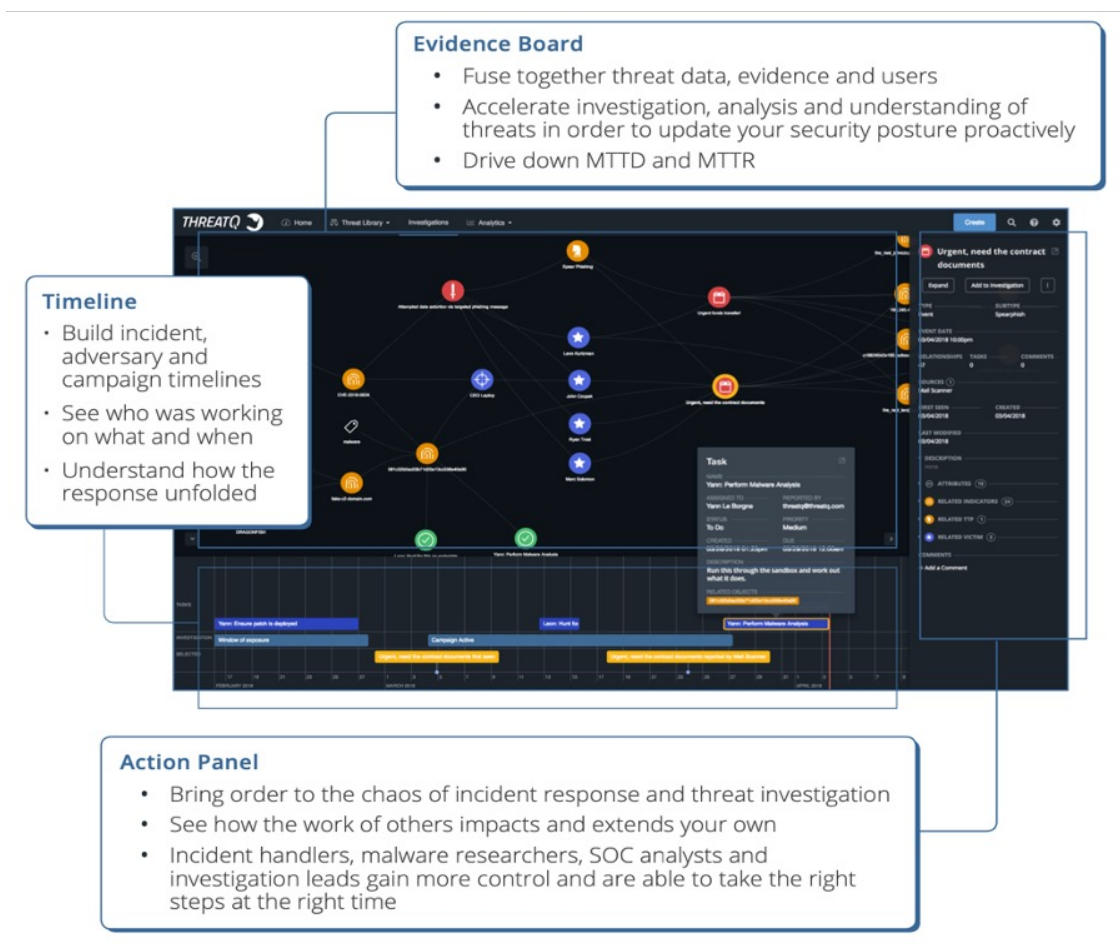
## 1.1 DEFINE ROLES AND RESPONSIBILITIES

### SAMA:

Member Organizations should define roles and responsibilities within the organization to produce threat intelligence with the expectation of creating their own CTI capability. This should include a dedicated team in charge of the production and dissemination of threat intelligence. In addition, the cyber threat intelligence team should be supported by skilled resources with purpose-specific advanced tools and a defined budget. Member Organizations should define communication channels inside the organization between the cyber threat intelligence team and other teams, including with stakeholders (e.g. Cybersecurity teams, business leaders, risk team, etc.) and with external organizations.

### ThreatQuotient:

ThreatQ provides a single central source of data on all relevant intelligence information from adversaries and vulnerabilities to tools and campaigns being tracked and defended against by the security teams. This allows ThreatQ to be the purpose-specific advanced tool specified by SAMA that all member organizations should provide to support the CTI team. Also, the intelligence data can be visualized clearly via dashboards and can serve to communicate the collected CTI to designated stakeholders.



(Note: image shows a sample ThreatQ dashboard used to visualize and communicate CTI)

## 1.2 DEFINE THREAT INTELLIGENCE PLANNING AND COLLECTION REQUIREMENTS

### SAMA:

Member Organizations should develop a set of threat intelligence requirements to guide their intelligence production efforts efficiently and to establish what intelligence should be produced to meet their security and business objectives. To define such requirements, Member Organizations should define the scope of the analysis (e.g. organizational, sectorial, national, etc.) and consider different areas of analysis relevant to their business priorities (e.g. technology, threat actors, etc.). In addition, Member Organizations should ensure periodical review of the defined requirements.

### ThreatQuotient:

Intelligence priorities and requirements can be tracked and shared through ThreatQ's data library which allows for the specific management of information relating to adversaries, campaigns and vulnerabilities that affect member organizations.

When used as a single source of intelligence data, ThreatQ can assist the CTI team in evaluating the threat data from different sources by providing the capability to ingest contextual data alongside indicators from these sources. Using ThreatQ's browsing and filtering capabilities, users can narrow down context from different areas of analysis (e.g. adversaries targeting specific industries and/or countries).

The screenshot displays the 'Data Management' interface with the 'Scoring' tab selected. Under 'Scoring Sensitivity Configuration', there is a description: 'Indicator scoring allows you to apply weighting to contextual information, such as sources, attributes, and indicator types. After scores are calculated, you can change the score as desired on the individual indicator pages. For each subset of data below, you can increase or decrease the score.' Below this, there are two configuration rows under the 'Attributes' tab. The first row is for 'Target Geography is Saudi Arabia' with a score of 3, and the second row is for 'Target Industry is Finance' with a score of 2. Each row has a slider from 'DECREASED' to 'INCREASED' and a 'Delete' button. A callout box on the right says 'Scoring Sensitivity by - GEO - SECTOR'. At the bottom, there is an 'Apply' button and a note: 'After clicking save, these changes will take time to process and will not immediately take effect.'

Indicator Type	Indicator Source	Attributes	Adversary Relationship
		Target Geography is Saudi Arabia	
DECREASED		3	INCREASED
			3 Delete
		Target Industry is Finance	
DECREASED		2	INCREASED
			2 Delete

**Scoring Sensitivity by**

- GEO
- SECTOR

**Apply** After clicking save, these changes will take time to process and will not immediately take effect.

(Note: image shows ThreatQ scoring capabilities for CTI)

## 1.3 SELECT AND VALIDATE RELEVANT SOURCES

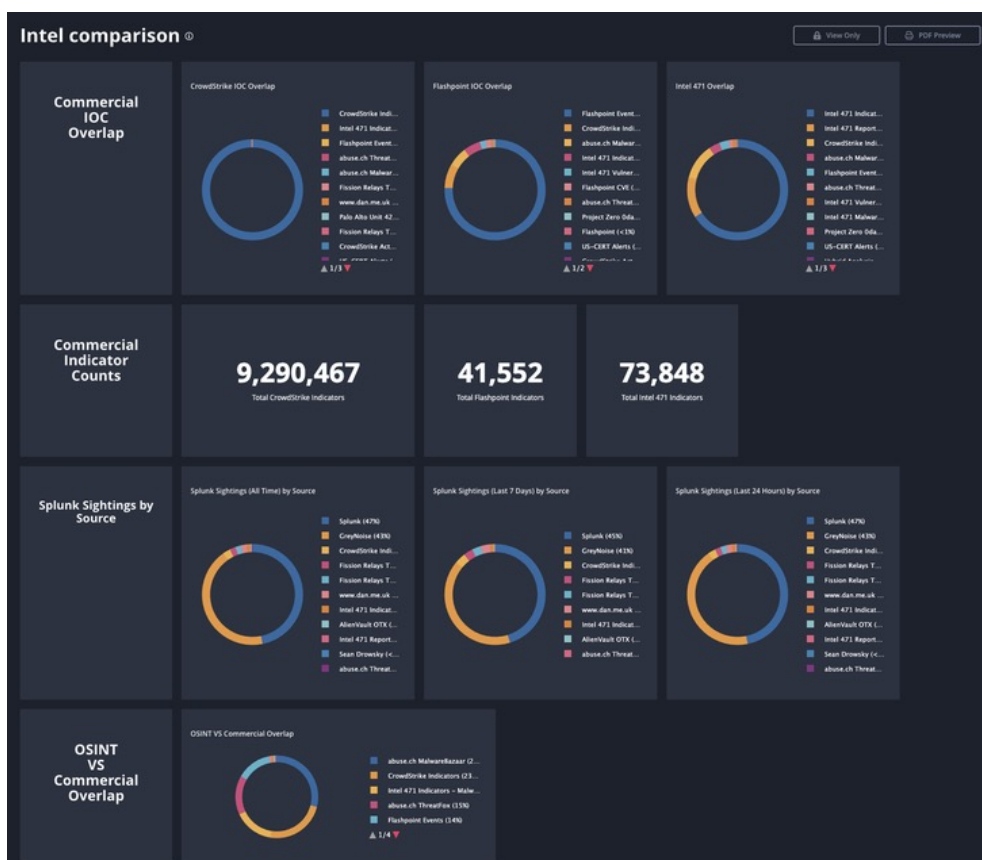
### SAMA:

Member Organizations should select sources in line with the defined threat intelligence requirements. Moreover, Member Organizations should define what type of sources to use, understand which sources are likely to produce the desired information, and consider a wide range of different sources to enable them to build a holistic understanding of threats relevant to the financial sector. Additionally, Member Organizations should assess the reliability and reputation of every source considering specific parameters. These parameters include the quality and accuracy of information, timeliness in relation to reporting, technical information included, comprehensiveness of threat feed, and type of information aligned with the defined threat intelligence requirements.

Member Organizations should select sources that provide information that is relevant to their business and in line with the threat intelligence requirements defined. These sources can be external or internal to the organization.

### ThreatQuotient:

Storing Intelligence data and applying scoring policy defined within ThreatQ allows for efficient usage of technical intelligence, and also allows member organisations to track the value of the feeds & sources they are using and make strategic decisions based upon the effectiveness of the data.



(Note: image shows a sample ThreatQ dashboard comparing CTI sources)

## 1.4 COLLECT DATA THROUGH INTELLIGENCE SOURCES

### SAMA:

Member Organizations should collect data via various intelligence sources (e.g. OSINT, TECHINT, SOCMINT, HUMINT and deep web and dark web intelligence). Gathering information from a diverse range of sources will produce holistic assessments of threats faced by the organization. Specific Standard Operating Procedures (SOPs) to conduct intelligence should also be followed.

### ThreatQuotient:

Feed collection, scoring and expiration are core elements of the ThreatQ platform. These provide the ability to collect threat intelligence from a wide variety of sources (e.g. OSINT, SOCMINT, commercial sources including deep and dark web amongst others) and ensure those which are of a higher priority can be acted upon swiftly.

ThreatQ has a rich ecosystem of integrations with 3rd party cybersecurity and CTI applications and sources. Currently, there are over 300 integrations that are available via the ThreatQ Marketplace, and new integrations are released on a weekly basis.

These integrations enable the collection of device data from network perimeter applications (e.g. alerts from SIEM, EDR, Firewall; malware sandbox analysis results; vulnerable assets discovered in vulnerability scans, etc.) as well as threat intelligence from OSINT and commercial sources.

The collection of external threat intelligence when combined with the internal network perimeter data, provide customers with a holistic view of the threats that could impact them and the activity within their own environment.

## Breadth of ThreatQ Ecosystem



(Note: image shows a representative sample of ThreatQ integrations; see [marketplace.threatq.com](https://marketplace.threatq.com) for a complete list)

## 1.5 DEFINE SPECIFIC STANDARD OPERATING PROCEDURES (SOPS)

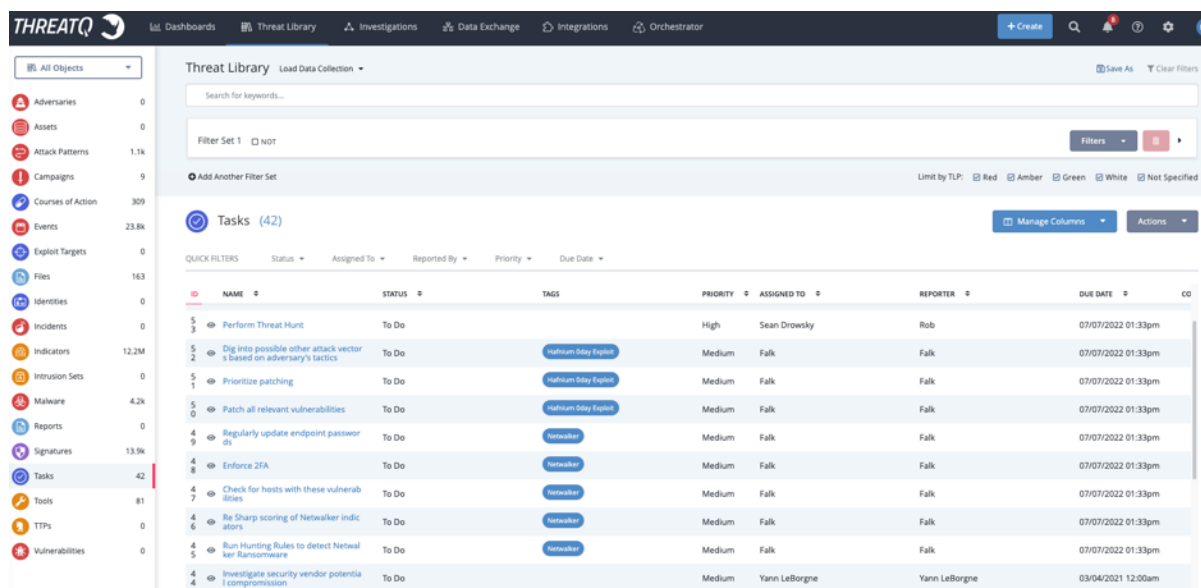
### SAMA:

Member Organizations should define specific standard operating procedures (SOPs) when conducting specific types of intelligence as detailed in “Principle 4: Collect Data Through Intelligence Sources”. Member Organizations should establish a set of instructions for individuals within the organizations to perform CTI to ensure functional procedures, while simultaneously reducing miscommunication and ambiguity. The SOPs should be detail-oriented and provide step-by-step instructions as to how analysts within Member Organizations must go about completing tasks and processes related to CTI.

### ThreatQuotient:

A central hub within the security stack can enable the Member Organization to build processes which include ThreatQ as the source or destination of information and actions. Tasking within the ThreatQ platform can aid with allocating and tracking work related to ongoing investigations and vulnerability management remediation as examples.

Member Organisations can build processes with ThreatQ that support SAMA's requirement for the reduction of miscommunication and ambiguity. Each Actor, Tools and Technique can have a single definition which can be linked to build relationships with other objects, but still updated independently to ensure that all information is pertinent and valid.



The screenshot displays the ThreatQ Threat Library interface. On the left is a sidebar with various object categories and their counts. The main area shows a 'Tasks (42)' list with columns for ID, NAME, STATUS, TAGS, PRIORITY, ASSIGNED TO, REPORTER, DUE DATE, and CO. The tasks listed are all 'To Do' and include actions like 'Perform Threat Hunt', 'Dig into possible other attack vectors', 'Prioritize patching', 'Patch all relevant vulnerabilities', 'Regularly update endpoint passwords', 'Enforce 2FA', 'Check for hosts with these vulnerabilities', 'Re Sharp scoring of Netwalker indicators', 'Run Hunting Rules to detect Netwalker Ransomware', and 'Investigate security vendor potential compromise'.

ID	NAME	STATUS	TAGS	PRIORITY	ASSIGNED TO	REPORTER	DUE DATE	CO
5	Perform Threat Hunt	To Do		High	Sean Drowsky	Rob	07/07/2022 01:33pm	
5	Dig into possible other attack vectors based on adversary's tactics	To Do	ThreatQ Delay Exploit	Medium	Falk	Falk	07/07/2022 01:33pm	
5	Prioritize patching	To Do	ThreatQ Delay Exploit	Medium	Falk	Falk	07/07/2022 01:33pm	
5	Patch all relevant vulnerabilities	To Do	ThreatQ Delay Exploit	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Regularly update endpoint passwords	To Do	Netwalker	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Enforce 2FA	To Do	Netwalker	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Check for hosts with these vulnerabilities	To Do	Netwalker	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Re Sharp scoring of Netwalker indicators	To Do	Netwalker	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Run Hunting Rules to detect Netwalker Ransomware	To Do	Netwalker	Medium	Falk	Falk	07/07/2022 01:33pm	
4	Investigate security vendor potential compromise	To Do		Medium	Yann LeBorgne	Yann LeBorgne	03/04/2021 12:00am	

(Note: image shows the ThreatQ Threat Library)



## 1.6 PROCESS AND CLASSIFY INFORMATION

### SAMA:

Member Organizations should process and classify collected intelligence - either manually, automatically, or a combination of the two - from the selected sources and store it securely. Furthermore, Member Organizations should refer to the “SAMA Cybersecurity Communication Protocols” when employing the Traffic Light Protocol (TLP) classification scheme for the collection and processing of information.

### ThreatQuotient:

ThreatQ utilizes TLP for the classification of information. Each source of data can be assigned a global TLP, and each individual piece of information can have its own TLP classification. This also applies to ThreatQ integrations for:

1. Collecting external threat intelligence from commercial and OSINT sources
2. Ingestion of network perimeter alerts and related indicators of compromise
3. Automating data processing and orchestration of actions

#### TLP (Traffic Light Protocol)

Disabled ☒ Enabled

TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience; it provides a method for designating the availability of intelligence information by their sources. TLP employs four colors to indicate expected sharing boundaries for data. [How it works](#)

Source Name	Default TLP
Filter by Source Name...	
aaron.brvenik@threatq.com	TLP Status <input checked="" type="radio"/> AMBER
abuse.ch Feodo Tracker Botnet C2 IP Blocklist	TLP Status <input type="radio"/> WHITE
abuse.ch Feodo Tracker Malware Hashes	TLP Status <input type="radio"/> WHITE
abuse.ch SSLBL IP Blacklist	TLP Status <input checked="" type="radio"/> GREEN
abuse.ch SSLBL Response Policy Zones (RPZ)	TLP Status <input type="radio"/> WHITE
abuse.ch SSLBL SSL Blacklist	TLP Status <input type="radio"/> WHITE
Accenture iDefense	TLP Status <input checked="" type="radio"/> GREEN
Accenture iDefense Campaigns	TLP Status <input checked="" type="radio"/> RED

(Note: image shows TLP classification within ThreatQ)

Depending on the deployment option chosen by a customer, data is stored securely in one of three ways:

1. Customer’s on-prem environment
2. Cloud-hosted, managed by the customer
3. ThreatQ’s hosted platform in an AWS, a SOC2 certified environment



## 1.7 ANALYZE INFORMATION

### SAMA:

Member Organizations should apply a variety of quantitative and qualitative analytical techniques to analyze the importance and implications of the processed information, and, in turn, produce actionable intelligence. Moreover, Member Organizations will combine and analyze various pieces of information, collected from diverse sources, to identify patterns, trends, and new developments relevant to the Member Organization.

Member Organizations should adopt adequate analytical approaches (e.g. Hypothesis-driven, Analyst-driven, and/or Contrarian) to be sure that the intelligence produced meets the intelligence requirements as defined in “Principle 2: Define Threat Intelligence Requirements”.

### ThreatQuotient:

Combining various pieces of information collected from diverse OSINT and commercial sources as well as information shared by peers and internally generated, plus patterns, trends, and new developments relevant to the organization can be managed through facilities within ThreatQ such as the Investigations Module and the Threat Library. Moreover, storing historical information in ThreatQ allows analysts to find historical patterns and understand if an indicator of compromise has been seen in the past within the organization.

Custom dashboards provide near-real time information about new threat intel and sightings & alerts within customers' environments.



(Note: image shows a sample ThreatQ dashboard configured for an XDR related use case)

## 1.8 SHARE INTELLIGENCE

### SAMA:

Member Organizations should establish specific sharing standards for the dissemination of threat intelligence. Member Organizations should establish a consistent and precise language practice throughout the organization to ensure wide applicability of threat intelligence. To clearly communicate threat intelligence, the Member Organizations should rely for example on a writing guide (e.g. the Economist Style Guide). They should also use a scale of 'estimative probability' system while engaging in analysis as defined in "SAMA's Threat Advisory Template".

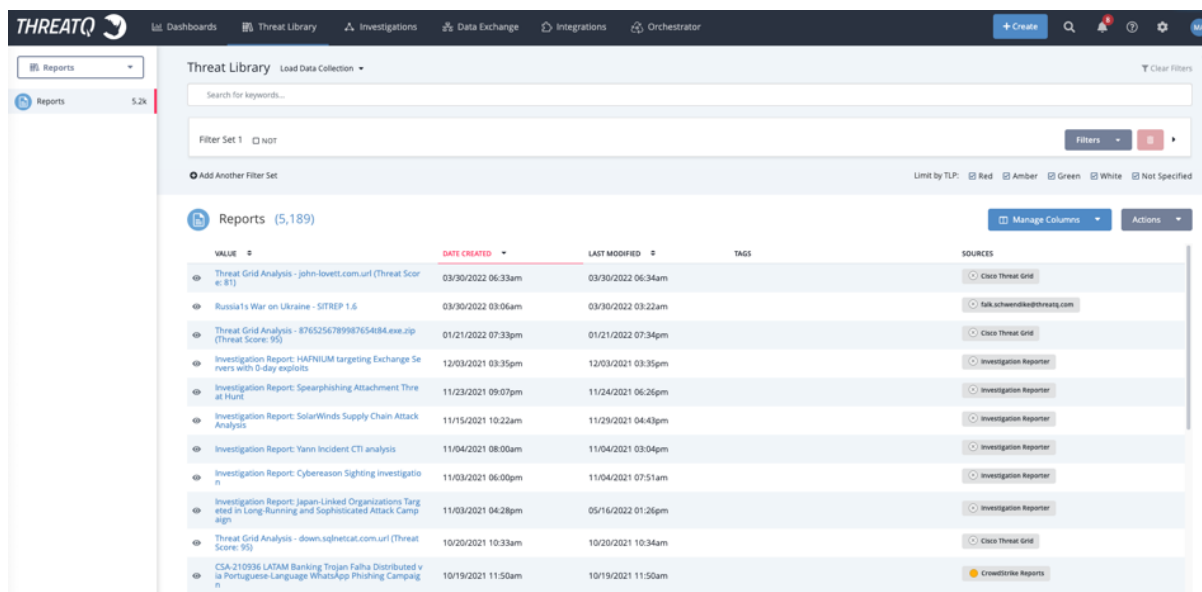
Member Organizations should disseminate threat intelligence in an effective, timely, and accurate manner. It should be presented in a clear, concise, and coherent way when shared with the relevant internal stakeholders. When sharing intelligence with SAMA, Member Organizations should define procedures that help control the publication and distribution of threat information.

All the information produced by the Member Organizations should be classified in accordance with the Traffic Light Protocol (TLP) classification scheme as per the "SAMA Cybersecurity Communication Protocols".

### ThreatQuotient:

ThreatQ provides functionality for sharing intelligence in different formats to internal and external stakeholders. ThreatQ offers API endpoints for ingesting and exporting information in a variety of formats (e.g. JSON, plain text, XML, STIX/TAXII, etc.).

Furthermore, ThreatQ offers native capability to expose data via URL endpoints and through custom integrations to export, transform and push the information to 3rd party applications. Additional sharing of the data is possible by generating reports by users via the web interface.



VALUE	DATE CREATED	LAST MODIFIED	TAGS	SOURCES
Threat Grid Analysis - john-lovett.com.url (Threat Score: 81)	03/30/2022 06:33am	03/30/2022 06:34am		Cisco Threat Grid
Russia's War on Ukraine - SITREP 1.6	03/30/2022 03:06am	03/30/2022 03:22am		tal.schwind@threatq.com
Threat Grid Analysis - 8765256789987654884.exe.zip (Threat Score: 95)	01/21/2022 07:33pm	01/21/2022 07:34pm		Cisco Threat Grid
Investigation Report: HAFNIUM targeting Exchange Servers with 0-day exploits	12/03/2021 03:35pm	12/03/2021 03:35pm		Investigation Reporter
Investigation Report: Spearphishing Attachment Threat at Hunt	11/23/2021 09:07pm	11/24/2021 06:26pm		Investigation Reporter
Investigation Report: SolarWinds Supply Chain Attack Analysis	11/15/2021 10:22am	11/29/2021 04:43pm		Investigation Reporter
Investigation Report: Yarovsk Incident CTI analysis	11/04/2021 08:00am	11/04/2021 03:04pm		Investigation Reporter
Investigation Report: Cyberreason Sighting Investigation	11/03/2021 06:00pm	11/04/2021 07:51am		Investigation Reporter
Investigation Report: Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign	11/03/2021 04:28pm	05/16/2022 01:26pm		Investigation Reporter
Threat Grid Analysis - down.safenetcat.com.url (Threat Score: 95)	10/20/2021 10:33am	10/20/2021 10:34am		Cisco Threat Grid
CSA-210936 LATAM Banking Trojan Falsa Distributed via Portuguese-Language WhatsApp Phishing Campaign	10/19/2021 11:50am	10/19/2021 11:50am		CrowdStrike Reports

(Note: image shows the ThreatQ Threat Library)

## 1.9 DELIVER ACTIONABLE THREAT INTELLIGENCE

### SAMA:

Member Organizations should implement relevant decisions and actions based on the intelligence produced to help build the resilience of the financial sector in the KSA. Member Organizations should take into consideration what actions are necessary, who is going to take these actions, and the response timeframe for anticipating or responding to an attack. Based on threat intelligence produced, Member Organizations should take relevant mitigation actions or measures to improve defense infrastructure and resilience based on their knowledge of relevant threats (e.g. knowing techniques adopted by threat actors on a network could help Member Organizations to prioritize mitigation controls).

The Member Organization's threat intelligence team should share relevant intelligence with other relevant departments such as the Security Operations Center (SOC), IT, etc. Sharing of such information should be done as per "Principle 8: Share Intelligence". These departments should also share information deemed relevant to the CTI capability as to feed and complement threat intelligence assessments.

### ThreatQuotient:

Through the use of integrations with 3rd party applications that are used to take mitigating actions such as blocking execution of files that match a hash, sending blocklists to a firewall or a proxy, quarantining a host on the network and more, ThreatQ can rapidly action technical intelligence.

Additionally, actions on 3rd party applications can be orchestrated using ThreatQ TDR Orchestrator. Moreover, relevant, and timely information including internally produced threat intelligence can be shared with internal CTI teams and other stakeholders via dashboards, email reports and threat feeds.



(Note: image shows a sample ThreatQ dashboard configured for an SOC related use case)

## 1.10 CONTINUOUSLY IMPROVE METHODS OF INTELLIGENCE

### SAMA:

Member Organizations should continuously maintain, update, and improve the production, processing, analysis, and dissemination of threat intelligence with the aim of continuously increasing the maturity of the financial sector in the KSA. Additionally, Member Organizations should also regularly update existing threat intelligence requirements based on feedback from internal and external stakeholders, threat intelligence users, changes in the industry, and evolutions within the global threat landscape.

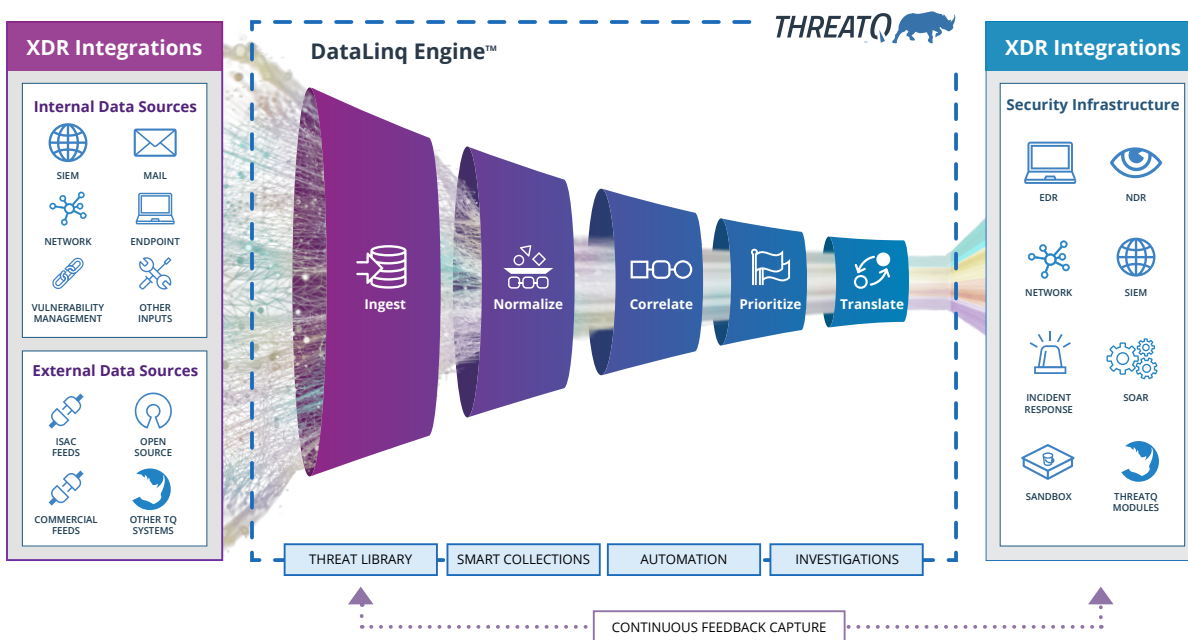
Member Organizations should perform periodic analysis of the threat information collected and verify its relevance (e.g. in terms of motivation, target, modus operandi, capability, etc.) according to assets and data processed by them. Member Organizations should also consider the services of a dedicated threat intelligence provider, who can offer relevant insights to complement the organization's existing understanding of threats.

Member Organizations should consider using Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), and Objectives and Key Results (OKRs) to quantify progress and update intelligence practices and protocols as aligned to their internal procedures.

### ThreatQuotient:

By being infinitely extensible in its features, data model and integrations, ThreatQ can evolve to support Member Organizations' security workflows as they expand and improve in line with SAMA recommendations.

Through the bi-directional integration with the internal tools, ThreatQ captures feedback from the internal tools and technologies which can then help in improving the CTI methods within the organization.



(Note: image shows a ThreatQ DataLinq Engine with feedback loop for continuous improvement)

## 1.11 INTEGRATE CTI

### SAMA:

Member Organizations should consider integrating CTI in situational awareness and red teaming assessments in line with the “SAMA FEER Framework”. The integration within situational awareness activities will help to build strategic understanding of cyber incidents, for example, identifying threat actors, trends in their activities, and objectives. Additionally, it will offer tactical understanding of events or situations in cyberspace and will facilitate effective and efficient decision-making in times of crisis.

Member Organizations should also take into consideration that the integration of CTI in red team assessment activities will help to get a better understanding of how cyber attackers gain access to networks and sensitive data. This can help to validate the organisation's security posture and help contextualise business process improvements by delivering more intelligence on cyber risks, their potential impact and remediation options.

### ThreatQuotient:

ThreatQ is equipped with integrations that can bring in the latest threat intelligence related to the Financial Sector industry in Saudi Arabia. Member Organisations have the flexibility to choose how they wish to incorporate the collected threat intelligence into red teaming assessments.



(Note: image shows a sample ThreatQ dashboard)

# 1.12 IDENTIFY A CYBER THREAT LANDSCAPE

## SAMA:

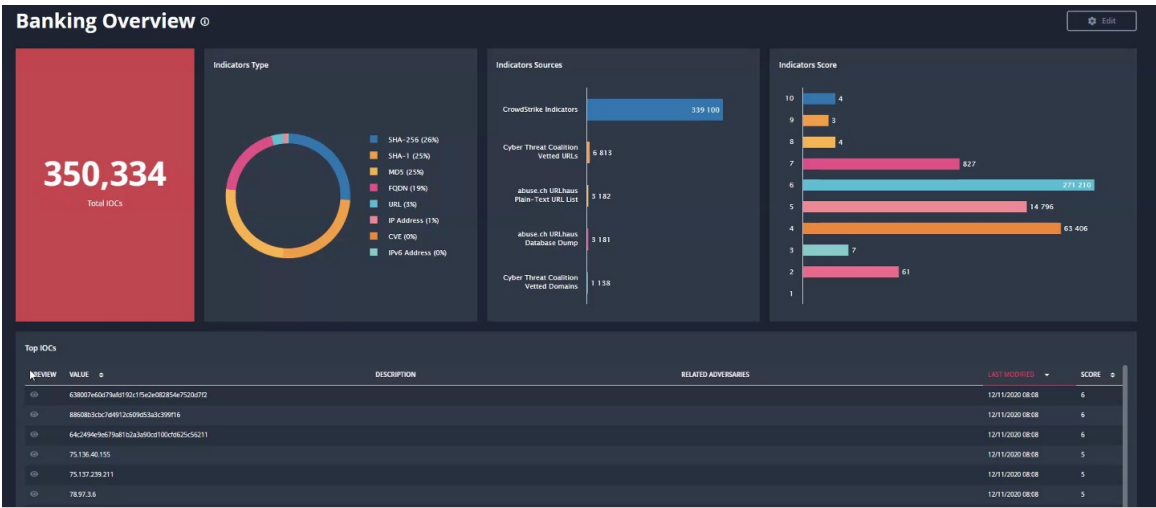
Member Organizations should identify the cyber threat landscape relevant to their organization and operations, with information on identified vulnerable assets, threats, risks, threat actors, and observed trends. This includes identifying events that can influence the financial sector’s threat landscape.

Moreover, Member Organizations should identify the threat actors that may intend to target them, and their main characteristics including their origin, intent, motivation, and capabilities. After identifying their threat landscape, Member Organizations should perform an assessment of the identified threats to prioritize which are the most relevant. Additionally, Member Organizations should also identify the main cyber trends that are likely to influence the future evolutions of the cyber threat landscape.

## ThreatQuotient:

Once the relevant parameters of a Member Organisation’s threat landscape have been identified these can be easily added to searches and dashboards within ThreatQ allowing for the tracking of vulnerabilities on internal assets, malware, tools and IOCs used by threat actors. Ingested threat intelligence contains context about target industries and target countries which can be utilized to identify relevant events in the threat landscape.

The scoring engine contained within ThreatQ enables Member Organizations to rapidly perform prioritisation of the mitigation for the results of regular assessment of the risks posed by discovered vulnerabilities.



(Note: image shows a sample ThreatQ dashboard)

### 1.13 IDENTIFY STRATEGIC CYBER ATTACK SCENARIOS

**SAMA:**

Member Organizations should identify the strategic cyber-attack scenarios that provide a realistic representation of likely cyber-attacks against them. These scenarios should involve one or more threat actors, address one or more targets, and the potential impacts of the scenarios.

To elaborate strategic cyber-attack scenarios, Member Organizations should identify similarities of features of threat actors or campaigns within the threat landscape outlined as per “Principle 12: Identify a Cyber Threat Landscape” (e.g. similar technique, similar attack type, etc.). In addition, Member Organizations should perform an assessment on the identified scenarios to prioritize the most likely and impactful scenarios and should take relevant corrective actions based on the threats and scenarios identified. The periodicity of the assessment of the identified scenarios should be defined by Member Organizations based on their own internal processes.

## ThreatQuotient:

ThreatQ provides the ability to record the actions and outcomes of previous attacks and combine these with additional information on the evolution of the threat landscape including campaigns and related adversary activities. Also, the ThreatQ Investigations Module can be used to visually map TTPs for attack scenarios.



(Note: image shows the ThreatQ Investigations Module user interface)



## 1.14 ELABORATE REQUESTS FOR INFORMATION (RFIS) AND TAILORED THREAT ASSESSMENTS

### SAMA:

Member Organizations should be able to provide, upon request, detailed information (e.g. cyber threats, trends, events, and malware or tools) related to possible cyber-attacks that could target them. These can be structured, for example, as threat actor profiles, country profiles, malware or tools analyses, or cyber trend studies.

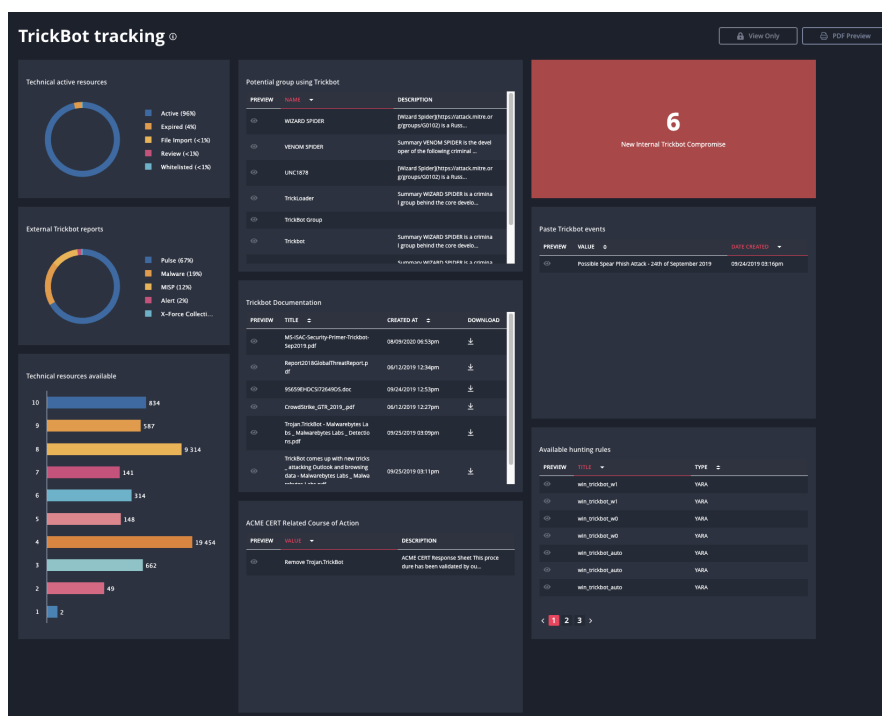
Member Organizations, based on the intelligence produced, should be able to perform tailored threat assessments to define the relevancy and level of potential threats, as well as the probability of attacks.

The CISO is responsible for validating the quality and relevance of the information. This information can be of particular interest to senior and executive management, business owners, owners of information assets, etc. This information is particularly valuable for instance when defining business strategies, planning security interventions, or following significant cyber incidents in the sector or in the country.

### ThreatQuotient:

ThreatQ provides the facility to store threats and trends based on incident related activity within the Threat Library. This not only allows for tracking and enrichment of all relevant intelligence gathered during incident response activities, but when this approach is applied rigorously within security operations processes it allows for significant simplification of the retrieval and dissemination of information.

Relationships between threat actors, malware, and tools they use, their TTPs, as well as the IOCs they have created builds the actors' profiles which can be sent via tailored custom reports to stakeholders at all levels.



(Note: image shows a sample ThreatQ dashboard configured for tracking a malware campaign)

## 1.15 DEFINE THE ATTACK CHAIN

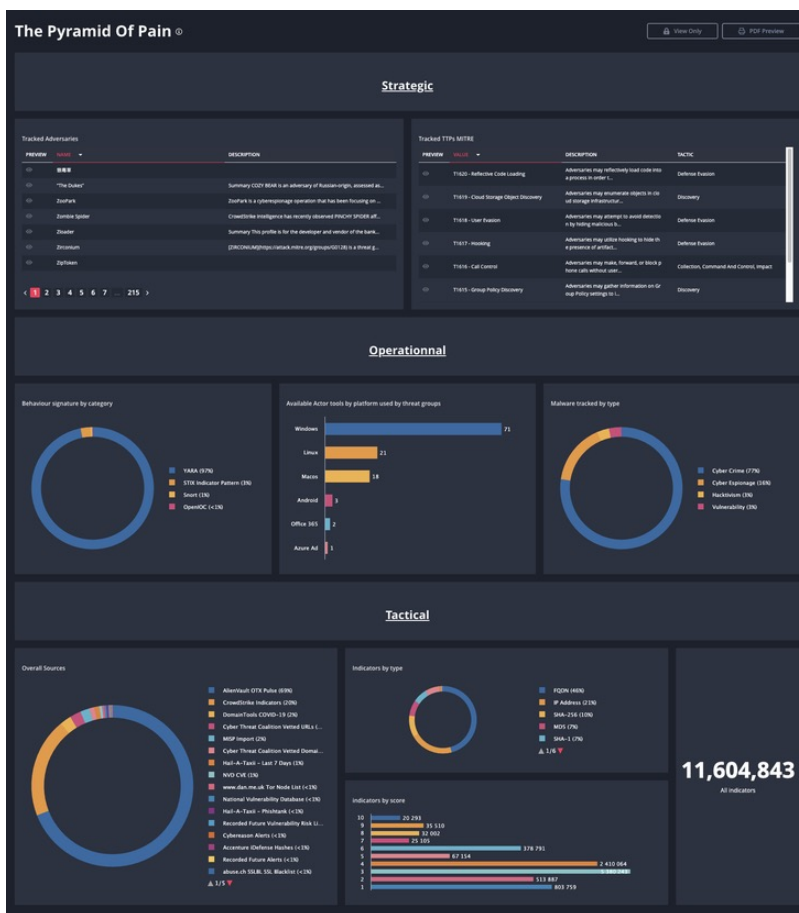
### SAMA:

Member Organizations should define and taxonomize the various phases of an attack performed by the threat actors based on industrial standards or frameworks (e.g. kill chain, unified kill chain, etc.). Moreover, Member Organizations should analyze information and modus operandi of the threat actors based on a structured approach to attacks (e.g. MITRE framework adopts a modified version of the unified kill-chain).

### ThreatQuotient:

ThreatQ's extensible data model allows for the full range of classifications and taxonomies used by various organizations. This extensibility alongside close integration with information sources such as MITRE's ATT&CK Framework, and agencies such as NIST's National Vulnerability Database (NVD), and CISA's Known Exploited Vulnerability Catalogue simplifies the ability to maintain and remain current on these elements.

The Threat Library's ability to provide a direct mapping to frameworks such as Lockheed Martin's Cyber Kill Chain and MITRE's ATT&CK also then allows analysts to relate events and indicators to the relevant point in the kill chain for tracking and later analysis.



(Note: image shows a sample ThreatQ dashboard)

## 1.16 IDENTIFY TTPS

**SAMA:**

Member Organizations should analyze the information collected from sources related to relevant threat actors, tools, or malware to identify relevant Techniques, Tactics, and Procedures (TTPs). In addition, Member Organizations should adopt a taxonomy of attacks and classification of such TTPs (e.g. MITRE ATT&CK). Based on the defined taxonomy, they should build threat actor behavior profiles and identify techniques used by threat actors. Member Organizations should rely also on Indicators of Compromise (IoCs) for the identification of these TTPs.

## ThreatQuotient:

Through the provision of objects specific to Techniques, Tactics, and Procedures for reference and updating these based on the changes in the threats, ThreatQ can relate these to adversaries and indicators amongst other objects to increase the context associated with the information.



(Note: image shows a sample ThreatQ dashboard)

## 1.17 IDENTIFY MALWARE AND TOOLS

### SAMA:

Member Organizations should identify malware and tools during an attack, as well as conduct a general classification of these to use at an organizational level (e.g. Banking Trojan, Ransomware, etc.). Member Organizations can obtain information regarding the different types of malware and tools used by the threat actors using different sources, such as Indicators of Compromises (IoCs), dark web, deep web, OSINT, code repositories, information sharing platforms, etc.

### ThreatQuotient:

The object-based model which is utilized by the ThreatQ Threat Library enables the classification and storage of specific artifacts based on their nature including adversary, tool, malware etc. These can also be related to each other to provide a full picture of all relevant objects and their relationships.

The screenshot displays the ThreatQuotient Malware 2.0 dashboard, which is organized into a grid of sections. Each section contains a detailed report or a list of indicators of compromise (IoCs) for a specific malware family.

- Conti:** A report on the Conti ransomware family, including a description of its operation and a list of IoCs.
- Squirrelwaffle:** A report on the Squirrelwaffle ransomware family, including a description of its operation and a list of IoCs.
- MirrorBlast:** A report on the MirrorBlast ransomware family, including a description of its operation and a list of IoCs.
- Avaddon:** A report on the Avaddon ransomware family, including a description of its operation and a list of IoCs.
- Ranzy Locker:** A report on the Ranzy Locker ransomware family, including a description of its operation and a list of IoCs.

Each report section includes a 'PREVIEW' tab and a 'VALUE' tab. The 'VALUE' tab displays a list of IoCs, each with a 'DATE' and a 'SCORE'.

(Note: image shows a sample ThreatQ dashboard configured for malware analysis)

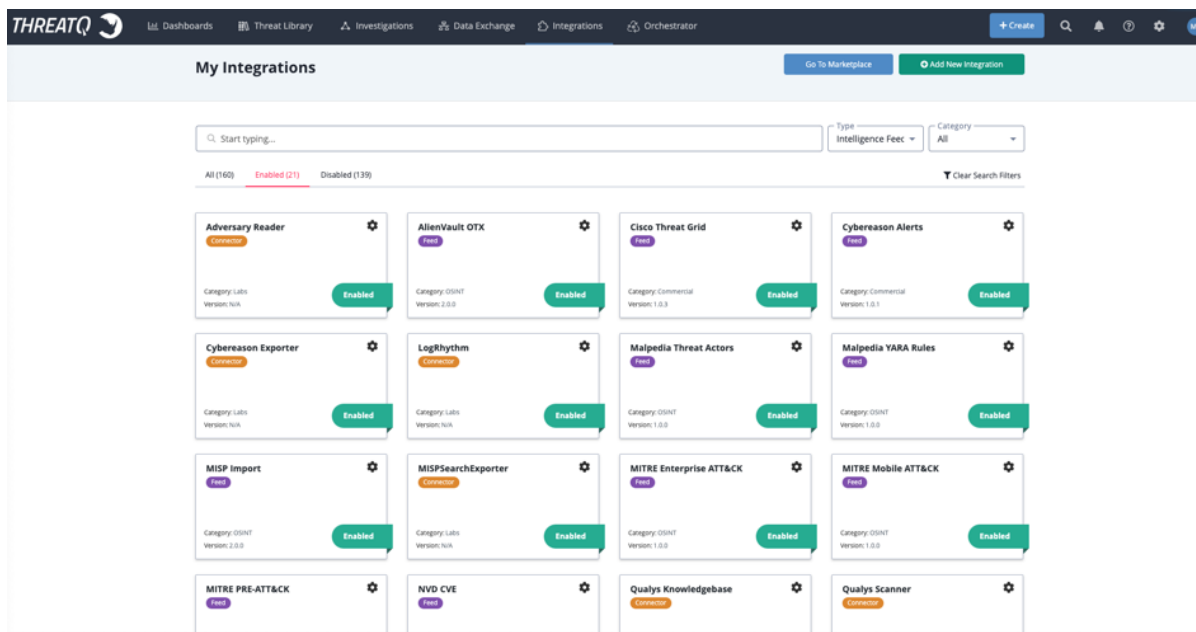
## 1.18 COLLECT IOCS

### SAMA:

Member Organizations should identify, collect, and aggregate IoCs and implement them in their defence infrastructure. Member Organizations should be able to collect details on specific implementation of malware and tools to understand how the organization is likely to be attacked and determine whether appropriate detection and mitigation mechanisms exist or whether they need to be implemented. In addition, Member Organizations should take into consideration different threat intelligence platforms and sources to obtain such technical information.

### ThreatQuotient:

ThreatQ's easy to use interface and multiple specific parsers make manual and automated collection, classification, and dissemination of IOCs simple. Feeds automate the mass collection of indicators from feeds, and integrations with technical controls allow for the ingestion of incident artifacts directly in some cases. ThreatQ offers more than 300 integrations which automate the ingestion of IOCs and contextual information. New integrations are released on a weekly basis.



(Note: image shows a ThreatQ integrations enabled for a sample deployment)

## 1.19 MONITOR AND REPORT VULNERABILITIES

### SAMA:

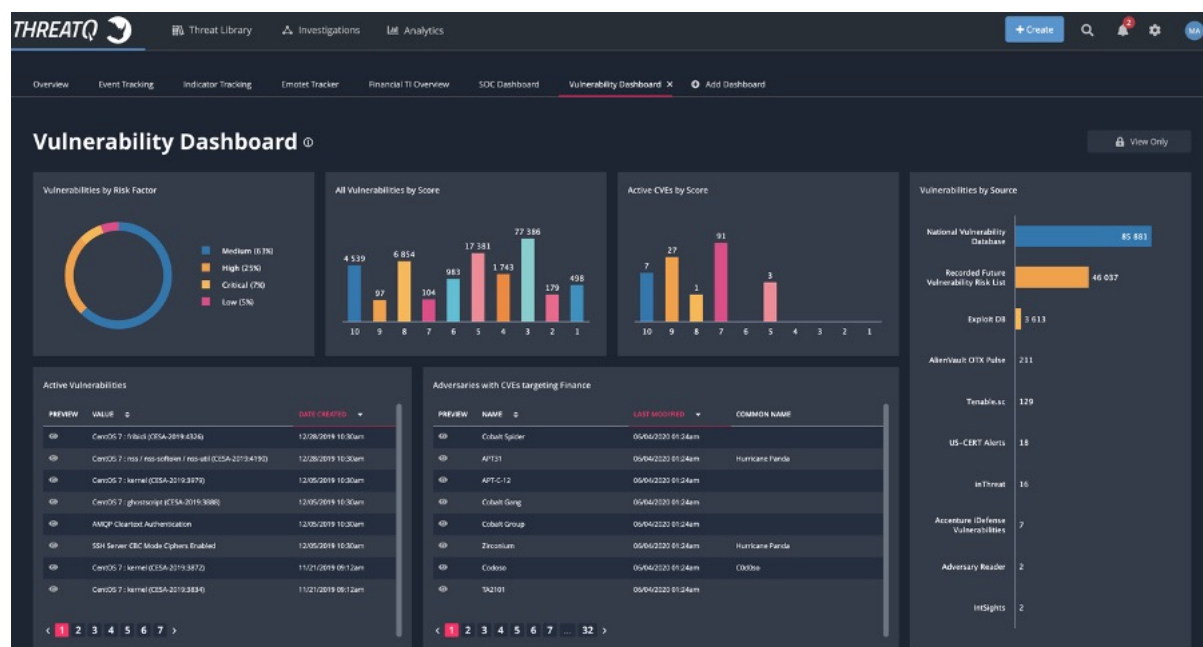
Member Organizations should constantly monitor announcements of new vulnerabilities discovered, as well as zero-day vulnerabilities exploited by threat actors. They should report these vulnerabilities to relevant parties within the organization (e.g. those in charge of patching management). These communications should be done in accordance to Member Organizations' internal procedures (e.g. SLA and KPI).

Member Organization should adapt a risk-based approach that correlates asset value, the severity of vulnerabilities, and threat actor activity via the use of threat intelligence and analytics to calculate a realistic risk rating. This rating should be used to prioritize remediation activities. In addition, Member Organization should use a risk-based approach to employ mitigating controls, such as intrusion prevention system (IPS), when unable to patch vulnerabilities to reduce the attack surface and prevent vulnerabilities from being exploited.

### ThreatQuotient:

ThreatQ's integrations with external OSINT and commercial threat intel providers (e.g. National Vulnerability Database, Intel471, Recorded Future, Mandiant, etc.) ingest known vulnerabilities. That information combined with integrations with Vulnerability Management tools (e.g. Qualys, Tenable.io, and Tenable.sc) show a complete picture of the known high-risk vulnerabilities that need to be patched and the hosts within the customer's estate that have those vulnerabilities.

Vulnerability Management teams within Member Organizations can use ThreatQ's data collections and dashboards to identify vulnerable assets, prioritize patching, and assign tasks to team members to complete required patching.



ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. For more information, visit [www.threatquotient.com](http://www.threatquotient.com).