تعميم

السادة/ المحترمون

السلام عليكم ورحمة الله وبركاته،

الموضوع: مبادئ تحليل التهديدات السيبرانية للقطاع المالي.

أشير إلى استراتيجية الأمن السيبراني للقطاع المالي الهادفة إلى خلق قطاع مالي آمن وموثوق يُمكّن من النمو والازدهار، ومن خلال متابعة التغير في نماذج الأعمال للمؤسسات المالية، والاعتماد على التقنية في المعاملات المالية، واستقطاب تقنيات ناشئة وحديثة.

عليه؛ فقد لوحظ تغير في مستوى التهديدات السيبرانية (Threat Landscape) للقطاع المالي والذي نتج عنه تطور سريع وملحوظ من قبل مجموعات الاختراق المتقدمة (Advance Persistence Threats "APT") التي تستهدف القطاع المالي لأغراض مختلفة وذلك على عدة أصعدة وأساليب وأدوات وإجراءات مستخدمة من قبلهم؛ مما يُحتِّم تطوير قدرات الرصد والتقصي للمؤسسات المالية للعمل بشكل استباقي يواكب تطور مجموعات الاختراق.

بناءً عليه، وانطلاقاً من دور البنك المركزي السعودي الرقابي والإشرافي على القطاع المالي؛ نحيطكم باعتماد مبادئ تحليل التهديدات السيبرانية للقطاع المالي (Financial Sector Cyber Threat Intelligence Principles) والتي تهدف إلى وضع أسس علمية وعملية للرصد والتقصي عن التهديدات السيبرانية وتعزيز ممارسات المؤسسات المالية في استقصاء التهديدات السيبرانية (Threat Landscape) لأخذ الإجراءات الاحترازية وتغذية مختلف الإدارات التقنية والتشغيلية وإدارات الأعمال بمعلومات استباقية (Threat Intelligence) تلائم عمل هذه الإدارات، حيث تم تقسيم المبادئ على عدة مستويات كالآتي:

- مبادئ أساسية – والتي يتطلب العمل بها كأساس لجميع عمليات الرصد والتقصي عن التهديدات السيبرانية.
- مبادئ استراتيجية – تركز على الجوانب الإستراتيجية للمعلومة المتقصَّى عنها مثل أهداف ودوافع مجموعات الاختراق وتحديد سيناريوهات الاختراق والهجوم المتوقعة حسب مستوى التهديدات السيبرانية للجهة والقيام بالتقييمات اللازمة.
- مبادئ تشغيلية – تستهدف تحليل الأنماط والأساليب التشغيلية لمجموعات الاختراق مثل البرامج الخبيثة والإجراءات المتبعة وتصنيف المراحل المختلفة للهجمات (Taxonomization).

- مبادئ تقنية – وهي المبادئ المتعارف عليها في تحليل التهديدات السيبرانية للخروج بمؤشرات الاختراق وضوابط الكشف والتصدي عن الهجمات السيبرانية.

عليه، ولتعزيز المرونة السيبرانية للقطاع المالي ورفع مستوى النضج للرصد والتصدي الاستباقي للتهديدات السيبرانية؛ فقد تقرر الآتي:

١. عمل تقييم دقيق للوضع الحالي لإدارة التهديدات الأمنية (Threat Intelligence) في المؤسسة المالية مقارنة بما ورد في المبادئ (Gap Assessment) بمختلف تصنيفاتها لتحديد الفجوات.
٢. وضع خطة عمل (Roadmap) للالتزام التام بالمبادئ اعتباراً من تاريخه، وذلك حسب المدد التالية:
   أ. ستة أشهر للمبادئ الأساسية والتشغيلية والتقنية.
   ب. اثنا عشر شهراً للمبادئ الإستراتيجية.
٣. يتوجب على المؤسسة المالية عرض الخطة المعدة (Roadmap) على مجلس الإدارة واطلاعهم عليها وأخذ الموافقة على الخطة والدعم اللازم لتطبيقها.
٤. على لجنة الأمن السيبراني في المؤسسة المالية متابعة تطبيق المبادئ ومدى الالتزام بالخطة المعتمدة وتقديم الدعم الكامل لحل العقبات والتحديات التي تواجه الفرق المختصة في المؤسسة المالية والتصعيد الداخلي لصاحب الصلاحية عن كل ما من شأنه أن يؤثر أو يعيق تطبيق المبادئ.

٥. يتعين على المؤسسة المالية تقديم الدعم اللازم لإدارة الأمن السيبراني لتطبيق كل ما ورد في الدليل وتعزيز دور تحليل التهديدات السيبرانية والتأكيد على تزويدهم بالكفاءات والكوادر الوطنية المدربة والأدوات التقنية والتدريب الملائم للقيام بمهامهم على أكمل وجه.

كما نود الإحاطة بأن البنك المركزي سيقوم بعمل زيارات إشرافية للتحقق من الالتزام التام بهذه المبادئ، وفي حال وجود استفسارات بهذا الخصوص يمكن التواصل مع الإدارة العامة للرقابة على المخاطر السيبرانية ممثلةً بالمركز الاستشرافي للأمن السيبراني على البريد الإلكتروني: (CFC@SAMA.GOV.SA).

وتقبلوا تحياتي،

فهد بن إبراهيم الشثري
وكيل المحافظ للرقابة

نطاق التوزيع:

- البنوك والمصارف المحلية والرقمية.
- شركة المدفوعات السعودية.
- شركات المعلومات الائتمانية.

مرفقات تعميم

مبادئ تحليل التهديدات السيبرانية للقطاع المالي.

رقم: ٤٣٠٦٥٣٤٨

تاريخ: ١٤٤٣/٠٧/٢٦هـ

Financial Sector
Cyber Threat Intelligence Principles

February 2022

Version 1

البنك المركزي السعودي
SAMA
Saudi Central Bank

Table of Contents

Introduction

With the progressive digitalization of financial services, safeguarding sensitive data, transactions, and the availability of services have become a priority to the financial sector in the Kingdom of Saudi Arabia (KSA). These services are not only fundamental to the global and national economy, but also vital to digital innovation and national security.

Cyber attacks have increasingly posed a significant challenge to organizations, with threat actors becoming more sophisticated and continuously evolving their modus operandi and attack vectors. Cyber Threat Intelligence (CTI) enables organizations to collect, analyze, and share data concerning cyber threats. A better understanding of these cyber threats, both existing and emerging, enables organizations to proactively anticipate cyber attacks and protect critical information assets.

The document is an extension of the Cyber Security Framework (CSF) mandated by the Saudi Central Bank (SAMA), specifically of its associated "Threat Management" subdomain. SAMA created the Cyber Threat Intelligence Principles with the aim of scaling up the CTI practices within the financial sector regulated by SAMA.

Scope of Applicability

This document is mandatory for all Member Organizations regulated by SAMA.

This document is intended for senior and executive management, business owners, owners of information assets, Chief Information Security Officers (CISO), and individuals accountable for and involved in defining, implementing, and reviewing Cyber Threat Intelligence within Member Organizations.

Responsibilities

This document is mandated by SAMA, who is the owner of the document and is responsible for its periodic updates. Member Organizations are responsible for adopting and implementing the principles contained in this document.

Review, Updates and Maintenance

SAMA will review the document periodically to evaluate its applicability to the context of the KSA financial sector and its Member Organizations. If deemed necessary, SAMA will update the document based on the outcome of the review. Once changes are applied, SAMA will retire the previous version, and release and communicate the new version to all Member Organizations.

Cyber Threat Intelligence Principles

The Cyber Threat Intelligence (CTI) Principles 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 through actionable threat intelligence.

The structure of the document has been developed based on different types of CTI. The principles contained in each section (Core, Strategic, Operational, and Technical and Tactical) have different purposes aiming at a holistic practice of CTI. In particular:

Core CTI Principles are a prerequisite to the practice of CTI and inform the other types of CTI. They include the activities needed to be performed for the planning, production, and dissemination of CTI.

Strategic CTI Principles involve a specialized CTI practice which include the activities needed to be performed for the identification of the objective, motivations, and intent of threat actors.

Operational CTI Principles involve a specialized CTI practice which include the activities needed to be performed for the identification of the modus operandi, behavior, and techniques used by threat actors.

Technical & Tactical CTI Principles involve a specialized CTI practice which include the activities needed to be performed for the identification of technical components and indicators of cyber attacks.

All principles should be applied by Member Organizations. The adoption of a phased approach for the complete implementation of the principles is at the discretion of the Member Organizations. The principles contained in this document apply also to the Member Organizations who outsource their CTI capability.

This document is organized in four domains including Core CTI, Strategic CTI, Operational CTI, and Technical and Tactical CTI as detailed in the graph below:

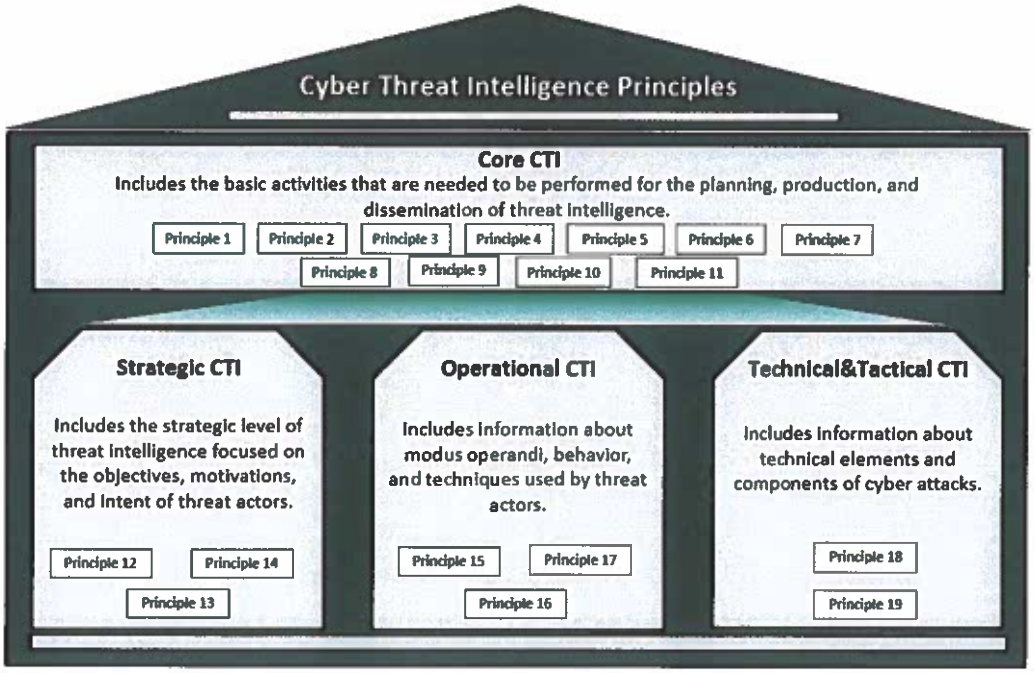


Figure 1. CTI Principles

Domain 1: Core Cyber Threat Intelligence Principles

Core Cyber Threat Intelligence Principles establish a baseline for the planning, collection, processing, analysis, and dissemination of threat intelligence based around the intelligence lifecycle framework.

The Core Threat Intelligence Principles section is based on the main phases of the intelligence lifecycle, including the dissemination of threat intelligence and continuously improving the CTI capability and performance of Member Organizations.

The intelligence lifecycle allows security teams to analyze and understand the information, prevent, and defend their networks from cyber attacks. It is the process by which raw data and information is identified, collected, and analyzed. Subsequently, raw data and information is transformed into intelligence to be used and actioned by Member Organizations. The intelligence lifecycle is fully represented by the following Core Principles.

Principle 1: Define Roles and Responsibilities

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.

Principle 2: Define Threat Intelligence Planning and Collection Requirements

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. *Further explanation of the areas of analysis is provided in "Annex B. Areas of Analysis".*

Principle 3: Select and Validate Relevant Sources

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. *Examples of internal and external sources are provided in "Annex C. Types of Sources".*

Principle 4: Collect Data Through Intelligence Sources

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. Examples of types of Intelligence are provided in *"Annex D. Types of Intelligence"*. Specific Standard Operating Procedures (SOPs) to conduct intelligence should be followed as specified in *"Annex F. Intelligence Standard Operating Procedures"*.

Principle 5: Define Specific Standard Operating Procedures (SOPs)

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. *Examples of SOPs are provided in "*Annex F. Intelligence Standard Operating Procedures*"*.

Principle 6: Process and Classify Information

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.

Principle 7: Analyze Information

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". *Examples of different types of analytical approaches are provided in "Annex G. Analytical Approach"*.

Principle 8: Share Intelligence

Member Organizations should establish specific sharing standards for the dissemination of threat intelligence. *Examples of delivery methods for threat intelligence are provided in "Annex E.- Threat intelligence Delivery Methods"*.

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".

Principle 9: Deliver Actionable Threat Intelligence

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.

Principle 10: Continuously Improve Methods of Intelligence

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.

Principle 11: Integrate CTI

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 assessments 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.

Domain 2: Strategic Cyber Threat Intelligence

Considering the changing nature of the threat landscape, Strategic CTI allows to continuously monitor the cyber ecosystem and to prevent threats.

Strategic CTI specifically helps at identifying and understanding the threats to the financial sector. It provides the level of threat intelligence focused on objectives, motivations, and intent of cyber threat actors. Strategic CTI aims at examining attribution, investigating real motivations and links between cyber events, and understanding the financial sector's ecosystem.

The threat landscape includes information on the threat actors that are most relevant to the Member Organizations, their main characteristics, and the main cyber trends within the financial sector worldwide.

This information is addressed to relevant executive management (e.g. Chief Information Security Officer) who will relay the information to other relevant parties (e.g. IT management, business leaders, etc.). Strategic CTI aids in the organization's understanding of current cyber threats, unknown future threats, threat actors, and attribution of attacks. Such understanding is key to having a pro-active approach to cybersecurity in order to build the resilience of the financial sector in the KSA.

Principle 12: Identify a Cyber Threat Landscape

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.

Principle 13: Identify Strategic Cyber Attack Scenarios

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.

Principle 14: Elaborate Requests for Information (RFIs) and Tailored Threat Assessments

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.

Domain 3: Operational Cyber Threat Intelligence

Operational CTI helps the Member Organizations to understand the nature, intent, and timing of a specific attack, and provides insight into the behavior of a threat actor on a network.

Operational CTI provides detailed information on the behavior and modus operandi of threat actors used to carry out cyber attacks. Generally, this information is commonly taxonomized in Tactics, Techniques, and Procedures (TTPs).

Principle 15: Define the Attack Chain

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).

Principle 16: Identify TTPs

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.

Principle 17: Identify Malware and Tools

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.

Domain 4: Technical and Tactical Cyber Threat Intelligence

Technical and tactical threat intelligence provide technical information regarding specific attacks performed by threat actors such as IoCs, Yara Rules, etc.

The indicators of technical threat intelligence are collected from active and past campaigns obtained from public sources, technical indicators collected within the organization, and/or data feeds provided by external third-parties.

Principle 18: Collect IoCs

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 in order 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.

Principle 19: Monitor and Report Vulnerabilities

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.

Annexes

Annex A. Glossary

The following list contains a definition of the main terms used in this document.

Glossary	
Term	**Description**
Application	A software program hosted by an information system. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Asset	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Attacker	Refer to "Threat actor".
(Threat actor) Capability	Resources and skills of a threat actor.
Cyber risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Cybersecurity	Cybersecurity is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the Member Organization's information assets against internal and external threats.
Cyber threat intelligence (CTI)	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
(Cybersecurity) Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Indicator of Compromise (IoC)	Indicators of compromise serve as forensic evidence of potential intrusions on a host system or network.

Glossary	
Term	**Description**
(Threat actor) Intent	The desire of a threat actor to target a particular entity. Threat actors are usually rational actors operating with a clear purpose (e.g. espionage, data theft/exfiltration, extortion, destruction, disruption, supply chain compromise).
Kill Chain	Adopted from the military, the kill chain was developer by Lockheed Martin to identify and taxonomize the various phases of a cyber attack (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions upon Objectives).
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. *Source: NISTIR 7298-3 Glossary of Key Information Security Terms*
MITRE ATT&CK	An open-source framework developed by MITRE taxonomizing tactics, techniques, and procedures used by threat actors when conducting cyber attacks.
Member Organization	Any regulated entity supervised and regulated by SAMA.
Modus Operandi	A method of procedure, especially referred to a distinct pattern or method of operation that indicates or suggests the work of a single criminal in more than one crime.
Motivation	The type of benefit or harm a threat actor ultimately wants to achieve with its actions.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. *Source: NISTIR 7298-3 Glossary of Key Information Security Terms*
Open Source Intelligence (OSINT)	Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements.
Organization	Company, entity, or group of people that works together for a particular purpose.
(Threat actor) Origin	Country from which the threat actor launches its attacks. The origin of a threat actor cannot always be determined with sufficient precision because they tend to cover their tracks.
Procedure	Procedures are the specific implementation the threat actor uses for techniques. *Source: MITRE ATT&CK*

Glossary	
Term	**Description**
Process	A set of interrelated or interacting activities which transforms inputs into outputs.
Ransomware	A form of malware designed to deny access to a computer system or data until ransom is paid. A user of a system infected with ransomware is usually confronted with an extortion message (in many cases a windows popup) asking the victim to pay a ransom fee to the threat actor (usually in cryptocurrency) in order to regain access to their system and data.
Red team (exercise)	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. *Source: NIST SP 1800-21B Glossary of Key Information Security Terms*
(Threat actor) Resources	Resources measure the scope, intensity, sustainability, and diversity of the total set of actions that a threat actor can take.
Sector	One of the areas in which the economic activity of a country is divided.
Service	A capability or function provided by an entity. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
(Threat actor) Skill	The extent to which a threat actor is able to leverage technical means (e.g. create custom malware) and operates with awareness, intelligence, learning potential, problem-solving, decision-making coherence, and operational experience.
Stakeholder	One who is involved in or affected by a course of action.
Strategic threat intelligence	The level of threat intelligence focused on objectives, motivations and intents of cyber threat actors. It aims at examining attributions to cyber threat actors, investigating real motivations and links between cyber events, and understanding complex systems dynamics and trends. Geopolitical, sectorial and context analysis is a fundamental tool.
Tactic	The threat actor's tactical goal: the reason for performing an action. *Source: MITRE ATT&CK*
(Threat actor) Target	The choices that actors make in terms of the target(s) of their attacks. A threat actor selects a target based on location, sector, and the types of information processed and attack surface available. The geopolitical landscape plays a key role in the targeting pattern of nation-state actors.
Taxonomy	A classification of interrelated elements.

Glossary	
Term	**Description**
Technique	Techniques represent "how" a threat actor achieves a tactical goal by performing an action. *Source: MITRE ATT&CK*
(Cyber security) Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. *Source: NISTIR 7298-3 Glossary of Key Information Security Terms*
Threat actor	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)" (NIST 2012) or, more in general, "An individual or a group posing a threat" (NIST 2016).
Threat landscape	A collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends. *Source: ENISA*
Threat intelligence requirement	Threat intelligence requirements guide the intelligence production effort efficiently and establish what intelligence should be produced to meet the security objectives of an Organization.
(Threat actor) Type	Grouping of threat actors who share similar characteristics, such as similar intents and motivations, and operate in similar ways.
Unified Kill Chain	An evolution of the kill chain framework detailing the phases of an attack.
(Attack) Vector	General approach for achieving an impact, taking advantage of the exposure of a type of, or a region in, an attack surface.

Annex B. Areas of Analysis

Member Organizations should develop threat intelligence requirements based on different areas of analysis which are relevant to their business priorities. These areas of analysis may vary depending on Member Organizations including but not limited to:

- **Geopolitics**: this includes requirements to identify geopolitical events that might determine a cybersecurity attack within the scope of analysis, such as large global campaigns carried out by threat actors, significant past relevant cybersecurity incidents, etc.
- **Threat actor:** this includes requirements to identify the main threat actors on which the organization should be particularly focused on.

- **Threat vectors:** this includes requirements to identify relevant attack techniques (e.g. initial access vectors, etc).
- **Technology:** this includes requirements to evaluate possible attacks against technologies that the organisation rely upon.
- **Industry:** this includes requirements to identify possible attacks against industries relevant to the organization (e.g. third parties in the supply chain or national critical infrastructure).

Annex C. Types of Sources

The following tables contain examples of internal and external sources.

Sources					
		Type of sources			
External sources	**Public sector**	Threat intelligence provided by SAMA and the National Cybersecurity Authority (NCA)	National civil or government bodies (e.g. law enforcement)	Reports or information from other sectorial or national authorities (e.g. CMA, FS-ISAC, Saudi CERT)	Public frameworks (e.g. ENISA, EUROPOL, MITRE)
	Private sector	Threat intelligence from specialized suppliers and platforms available upon subscription or contract	Publicly available threat intelligence reports, news, briefs and analyses		
	Academic sector	Whitepapers	Academic publications and conferences	Academic journals	

Table 1. External sources

Sources	
	Type of Sources
Internal sources	Application and infrastructure logs
	Intrusion Detection System (IDS)
	Intrusion Prevention System (IPS)
	Cyber security defence systems

Table 2 Internal sources

Annex D. Types of Intelligence

Currently, there is a wide range of different kinds of intelligence that could be used to obtain a holistic understanding of the threats that an organization faces.

These types of intelligence include:

- **OSINT**: open source intelligence obtained from publicly available sources (e.g. Threat report, blog, etc.)
- **TECHINT**: technical intelligence derived from signals generated routinely by hardware devices or software applications connected to an organization's network (e.g. IoCs, malware analysis, code reports, etc.)
- **SOCMINT:** social media intelligence, a process of identifying, gathering, validating, and analyzing data from social media sites and accounts (e.g. Blogs, microblogs, social networks, etc.)
- **HUMINT:** human intelligence derived overtly or covertly from human sources based on a relationship between an intelligence analyst and the analyst's handler (e.g. active monitoring on forums)
- **Deep and Dark Web Intelligence:** intelligence gathered on the deep and dark web (e.g. marketplaces, forums, etc.)

Annex E. Threat Intelligence Delivery Methods

Member Organizations should establish the delivery mechanism of the threat intelligence produced which includes, but is not limited to:

- **Cyber threat bulletins** including cyber threat information that may be useful for the organizations
- **Simple alerts** sent out by phone, text, or email
- **Detailed reports** enriched with analysis, tables, numbers, graphics, and multimedia
- **Machine-readable data feeds** based on a proprietary or open standard structured threat intelligence notation, for Security Information and Event Management (SIEM), anti-virus software, firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS) and forensic tools
- **Custom-designed output** for in-house systems
- **Application Programming Interfaces (APIs)** enabling direct system connection for the purposes of intelligence query or retrieval
- **Secure online portals** providing on-demand access to an up-to-date threat intelligence database and a range of analytical functions that could be as basic as from simple queries to more complex data mining

Annex F. Intelligence Standard Operating Procedures

Below are listed some examples of how SOPs should help users when performing specific kind of threat intelligence.

When performing deep and dark web intelligence, the step-by-step instructions should help users in identifying all the elements needed to properly conduct it, including but not limited to:

- Using a controlled isolated and untraceable environment such as a Virtual Machine (VM)
- Update and collect a list of deep web and dark web forums and marketplaces
- Create various avatars for access

Similarly, when performing Social Media Intelligence (SOCMINT), the step-by-step instructions should help in identifying all the elements needed to properly conduct it, for example:

- Providing users with a list of different types of sources and continuously updating this list (e.g. Blogs, microblogs, social networks, images, video, and discussion forums)
- Conduct training on Social network and online video hosting and sharing platform (e.g. Twitter, Facebook, YouTube etc.)
- Using social media tools when possible (commercial and open-source)

In the same way, when performing human intelligence (HUMINT), the step-by-step instructions should help users in identifying all the elements needed to properly conduct it, including but not limited to:

- Conduct ethics training for analysts performing active engagements online
- Implement SOPs related to forum and marketplace accesses
- Build an avatar for each access to avoid traceback
- Understanding the difference between active and passive monitoring

Annex G. Analytical Approach

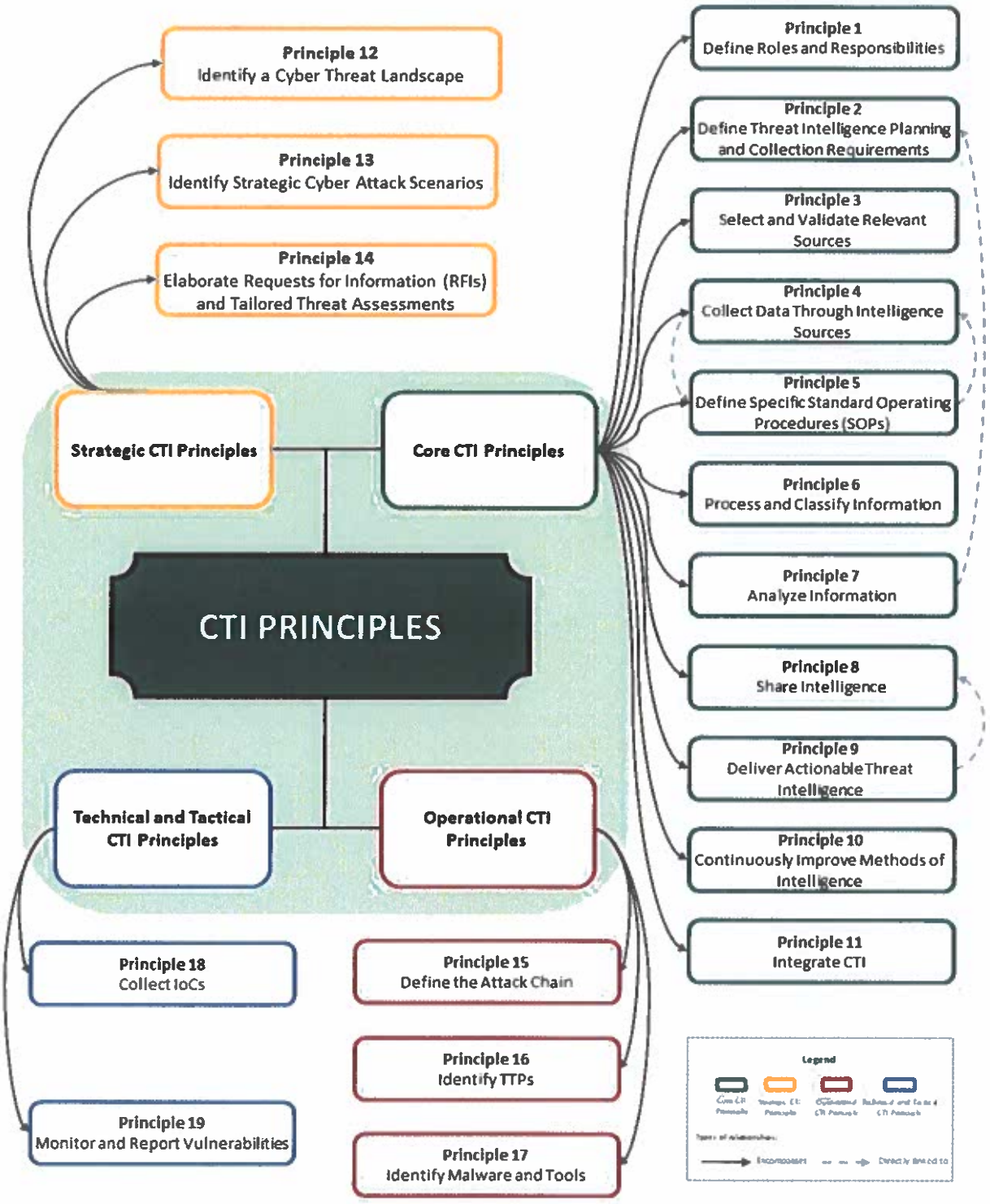
Member Organizations should adopt an analytical approach so the intelligence produced meets the intelligence requirements.

Based on what is most suitable for the Member Organizations, the analytical approach could be:

- **Hypothesis-driven**: this approach includes the definition of a hypothesis and its evaluation by analyzing available information
- **Analyst-driven**: this approach is based on the analyst's critical and analytical thinking
- **Contrarian**: this approach aims at challenging the main conclusions or points made by the source to put forward a counter-argumentative approach

Annex H. CTI Principles High-Level Graph

Below is represented a high-level graph of the CTI principles. The graph is aimed at representing the high-level structure of the document.


Principle 12
Identify a Cyber Threat Landscape
Principle 13
Identify Strategic Cyber Attack Scenarios
Principle 14
Elaborate Requests for Information (RFIs) and Tailored Threat Assessments
Strategic CTI Principles
Core CTI Principles
CTI PRINCIPLES
Technical and Tactical CTI Principles
Operational CTI Principles
Principle 18
Collect IoCs
Principle 19
Monitor and Report Vulnerabilities
Principle 15
Define the Attack Chain
Principle 16
Identify TTPs
Principle 17
Identify Malware and Tools
Principle 1
Define Roles and Responsibilities
Principle 2
Define Threat Intelligence Planning and Collection Requirements
Principle 3
Select and Validate Relevant Sources
Principle 4
Collect Data Through Intelligence Sources
Principle 5
Define Specific Standard Operating Procedures (SOPs)
Principle 6
Process and Classify Information
Principle 7
Analyze Information
Principle 8
Share Intelligence
Principle 9
Deliver Actionable Threat Intelligence
Principle 10
Continuously Improve Methods of Intelligence
Principle 11
Integrate CTI
Legend

Annex J. CTI Principles Mind Map

Below is represented a mind map of the structure of the CTI principles. The graph is aimed to clearly represent the different domains of the document and how the principles are related to each other.