Resecurity

Cyber Threat Intelligence (CTI) for Financial Institutions

Compliance with SAMA Framework and regulatory requirements

Applying Cyber Threat Intelligence and the SAMA Framework to Secure Saudi Arabian Financial Institutions

Benefits of cybersecurity intelligence solutions to meet compliance

Introduction

In line with Saudi Arabia's Vision 2030 program, the Kingdom of Saudi Arabia (KSA) has invested heavily in its digital transformation and combating the emerging cyber threats that have come with it - particularly around the financial services sector in KSA. As a critical part of KSA's digital economy, innovation and security, safeguarding financial services is essential to ensure sensitive data, transactions and support continue without being disrupted.

To help protect financial services essential to the economy, KSA and the Saudi Central Bank (SAMA) mandated a Cyber Security Framework (CSF) regulating the cybersecurity practices of SAMA's financial organizations (Member Organizations). With growing cyber risks targeting the financial sector, SAMA recently issued a new Threat Management subdomain of the CSF and underlying Cyber Threat Intelligence Principles (CTIs) in March 2022.

This whitepaper explores what the CSF Framework and new CTIs mean for KSA financial service providers, as well as existing threat intelligence solutions that can help organizations meet SAMA compliance.

The role of the SAMA Framework

SAMA, the central bank of KSA and the heart of its economy, is responsible for issuing national currency, supervising commercial banks, operating digital financial systems, ensuring stability of KSA's financial system and more. To support economic prosperity, SAMA also issues governance and regulations for financial institutions in KSA. In 2017, SAMA published the CSF to provide a consistent security framework and regulations for SAMA's financial institutions, protecting the critical data and systems they house.

Within the Framework, cyber security 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".

Adapting to the latest cyber threats, threat actors and threat intelligence best practices, SAMA has created the Cyber Threat Intelligence Principles with the aim of scaling up threat intelligence practices within the financial sector regulated by SAMA.

Understanding Cyber Threat Intelligence Principles

The Cyber Threat Intelligence (CTI) Principles are best practices to help financial organizations adequately implement a new age of threat intelligence, detection and response tactics to enhance the identification and mitigation of cyber threats relevant to the financial sector. All SAMA members will be required to apply the CTI principles.

The 19 CTI principles are broken into four domains including:

1. CORE CTI PRINCIPLES
(Principles 1-11)

Key principles that are the foundation for the planning and production and implementation of CTI. Example principles include: define roles and responsibilities, process and classify information, analyze information and deliver actionable threat intelligence.

2. STRATEGIC CTI PRINCIPLES
(Principles 12-14)

CTI activities related to the identification of the objective and motivations of threat actors. Example principles include: identify a cyber threat landscape and elaborate requests for information and tailored threat assessments.

3. OPERATIONAL CTI PRINCIPLES
(Principles (15-17)

CTI activities related to detection of behaviors and techniques used by threat actors.Example principles include:define the attack chain, identify TTPs and identify malware and tools.

4. TECHNICAL & TACTICAL PRINCIPLES
(Principles 18-19)

CTI activities related to the identification of technical indicators of a cyber incident. Example principles include: collect IoCs and monitor and report vulnerabilities.

How CTI Can Help Enterprises Mitigate Cyber Risks

Financial organizations who successfully implement the CTI principles mandated by SAMA will benefit from actionable threat intelligence that improves visibility into their security ecosystem, provides key data about threat actors and landscapes, facilitates tailored defense strategies, and enables teams to respond to security incident response faster or better yet, prevent incidents from happening in the first place.

While the CTI principles will improve the security posture of SAMA members, security leaders can expect a significant investment of resources to add this layer of threat intelligence, detection and response. To mitigate the additional time and staff that will be needed to implement the CTI principles, organizations should consider advanced threat intelligence tools that meet and support many of the principles outlined by the SAMA framework.

Resecurity www.resecurity.com info@resecurity.com (800) 781-5698 445 S. Figueroa Street, 31st Floor, Los Angeles CA 90071, USA

The Advantages of Resecurity's Threat Intelligence Platform

For SAMA financial institutions needing to scale threat intelligence capabilities quickly, Resecurity's cyber threat intelligence platform, Context™, not only accelerates analysis, prevention and investigation workflows with lightning-fast search and data science but contextualizes threat data to make it clear and actionable. Through Context™, security teams can transform from managing many streams of raw intelligence and false positives to leveraging a single tool that provides a one-stop-shop for comprehensive threat intelligence data and real-time insights. Context™ allows financial organizations to create their own cyber threat intelligence center or cyber fusion center and to accelerate operations of their SOC.

Aligned to the Intelligence Lifecycle used to create the CTI principles, Context™ follows the same six-step process to provide a balanced and comprehensive approach to threat intelligence gathering and analysis. Tapping into 5 billion data points and using industry-leading data science, the platform allows administrators to reduce potential blind spots and security gaps by quickly seeing in-depth analysis and specific artifacts obtained through the dark web, botnets activity, network intelligence and high-quality threat intelligence data.

How Resecurity Can Help You Meet SAMA Framework Requirements

As financial organizations look to implement the CTI principles and SAMA framework, Context™ is a complementary and cutting-edge platform that can help get them to compliance and security faster. In the scope of SAMA Framework, Resecurity's threat intelligence platform delivers:

- Actionable cyber threat intelligence and feeds related to the financial sector consumed from over 35,000 data points,
- Indicators of compromise (IoCs) related to online banking and e-commerce malware targeting customers in KSA,
- Proactive alerts describing new threat actors, cybercriminal groups and their Tools, Tactics and Procedures (TTPs) used in cyberattacks,
- Assistance and expert support with threat intelligence briefings designed by Certified Cyber Threat Intelligence Analysts,
- Human intelligence (HUMINT) services and investigative support to conduct an in-depth analysis of the malicious activity.

Conclusion

Cyber Threat Intelligence (CTI) is a vital component of modern cybersecurity operations. New SAMA CTI principle regulations are an exciting step towards securing KSA's digital economy and the financial services critical to future growth and innovation. Accordingly, security leaders at financial institutions must adapt and leverage the latest cybersecurity intelligence and tactics, quickly and at scale. For financial organizations looking to partner with threat intelligence experts local to KSA and familiar with the CTI principles, they can feel confident that leveraging the Context™ platform will help them meet SAMA compliance and mitigate business risk.