Darktrace and the SAMA Cyber Security Framework

Introduction

Responding to the growing challenge that cyber risk poses to the financial sector, the Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework aims to articulate appropriate controls, assessment methods, and security practices to ensure that Saudi Arabian financial services companies can manage and withstand cyber security threats.

The framework, based on industry-leading cyber security standards and practices, has three key objectives:

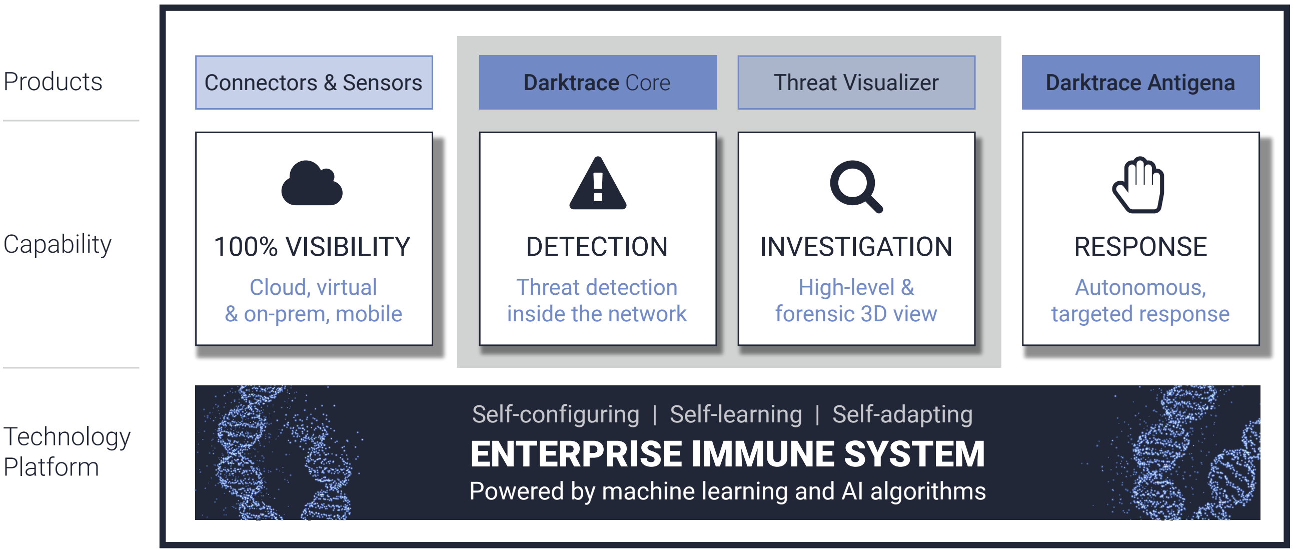
- Create a common approach for addressing cyber security
- Achieve an appropriate maturity level of cyber security controls
- Ensure cyber security risks are properly managed

All SAMA Member Organizations will be required to follow the provisions of the framework. This includes all banks, insurance and reinsurance companies, financing companies, credit bureaus, and financial market infrastructure.

No single solution can fulfill all of the framework's requirements, and **"the ultimate responsibility for cyber security rests with the board of the Member Organization."** Regulations vary, from governance structures and vendor relations, to physical entry controls and surveillance. Non-compliance is expected to result in significant penalties.

> "With Darktrace, we know that our firm's financial data is secure."
>
> AEA

This white paper demonstrates how Darktrace's world-leading cyber AI addresses the most challenging obligations of the SAMA Cyber Security Framework, enabling organizations to reach the regulation's highest security rating of Level 5. Darktrace's AI provides threat detection and autonomous response across the entire digital infrastructure, allowing businesses to get ahead in the race to secure their systems and providing the solid foundation for the construction of your critical cyber security policies.


Products
Capability
Technology Platform
Connectors & Sensors
Darktrace Core
Threat Visualizer
Darktrace Antigena
100% VISIBILITY
Cloud, virtual & on-prem, mobile
DETECTION
Threat detection inside the network
INVESTIGATION
High-level & forensic 3D view
RESPONSE
Autonomous, targeted response
Self-configuring | Self-learning | Self-adapting
ENTERPRISE IMMUNE SYSTEM
Powered by machine learning and AI algorithms

> “With Darktrace, talk about AI in cyber security has turned into action.”
>
> Ovum

Framework Objectives

The purpose of the SAMA Cyber Security Framework is defined as: **“to enable Financial Institutions regulated by SAMA […] to effectively identify and address risks related to cyber security.”** It was enacted in May 2017 and will come into effect on October 31st, 2018.

The provisions of the framework are wide-ranging, affecting domains well beyond those traditionally associated with cyber security. It ensures that cyber security is integrated into every aspect of corporate governance, planning, and policy.

SAMA lists the general security objectives of the framework as follows:

- **Confidentiality** – Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data).
- **Integrity** – Information assets are accurate, complete and processed correctly (i.e., protected from unauthorized modification, which may include authenticity and non-repudiation).
- **Availability** – Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).

The framework defines information assets as: “Electric information, physical information (hardcopy), applications, software, electronic services and databases, computers and electronic machines (e.g. ATM), information storage devices (e.g. hard disk, USB stick), premises, equipment and communication networks (technical infrastructure).”

AI for SAMA Compliance

Darktrace’s artificial intelligence has been adopted by some of the largest companies in global finance, such as Allianz and AIG, in their efforts to stay ahead of both the regulator and the threat landscape. It will quickly prove vital to SAMA regulated organizations in their efforts to comply with the far-reaching demands of the new framework.

SAMA has placed specific emphasis on organizations’ resilience to threats, focusing on their ability to identify, analyze, respond, monitor, and review risks. All of these functions are intrinsic to Darktrace’s AI for cyber defense.

Powered by AI, Darktrace’s Enterprise Immune System, forms a ‘pattern of life’ that characterizes each network, device, and user, allowing it to detect and respond to emerging threats wherever they appear across the digital estate. When malicious activity is identified, Darktrace’s autonomous response solution – Darktrace Antigena – then takes precise, surgical measures to fight back against in-progress threats within seconds.

Darktrace’s intuitive user interface, the Threat Visualizer, allows security teams to visualize all digital activity and investigate anomalies in real time. As well as Darktrace’s real-time threat detection and response, users can also replay an incident to understand how it unfolded, viewing all historical logs and events.

Darktrace’s ability to provide total visibility and real-time AI defense will prove crucial in complying with the framework’s key conditions: preserving the confidentiality, availability and integrity of information assets. Critically, Darktrace’s Enterprise Immune System adapts and ‘grows’ with your organization, learning about every device, user, and the network as a whole, no matter the size and complexity. This includes IoT, BYOD, payment systems, the cloud, and SaaS.

Darktrace’s visualization capabilities can also be used to provide a high-level overview of a company’s systems to the board. Executives are given oversight of security issues, improving their awareness and understanding of the digital environment, and enhancing their ability to make better-informed managerial decisions.

Furthermore, Darktrace offers a range of services which facilitate corporate governance of the cyber security process. These include weekly Threat Intelligence Reports, on-demand Executive Threat Reports, Darktrace training programs, Industry Trend Reports, and Global Threat Notifications.

Reaching Maturity Level 5: Darktrace & Self-learning Cyber AI

The best way to assure compliance with the Cyber Security Framework is to attain Maturity Level 5, the highest security rating as defined by SAMA.

> "Maturity level 5 focuses on the continuous improvement of cyber security controls. Continuous improvement is achieved through continuously analyzing the goals and achievements of cyber security and identifying structural improvements. Cyber security controls should be integrated with enterprise risk management practices and supports with automated real-time monitoring. Business process owners should be accountable for monitoring the compliance of the cyber security controls, measuring the effectiveness of the cyber security controls and incorporating the cyber security controls within the enterprise risk management framework. Additionally, the performance of cyber security controls should be evaluated using peer and sector data."

To achieve this, organizations need the most sophisticated, proactive cyber defense measures, which take advantage of the latest developments in cyber AI. Darktrace's Enterprise Immune System integrates into existing security stacks with ease and will help businesses to fulfill Level 5's requirements.

Unlike static, rule-based defenses, Darktrace's self-learning AI technology offers **"continuous improvement of cyber security controls."** The longer it is deployed, the stronger the protection it offers your enterprise. Darktrace's unique application of unsupervised machine learning means that it learns 'on the job', without making assumptions about what is 'malicious' or otherwise.

The total visibility provided by the Enterprise Immune System is essential for **"identifying structural improvements."** Darktrace AI also uncovers the unforeseen vulnerabilities which legacy tools miss, particularly in non-traditional IT, such as third-party internet-connected devices and cloud systems. Whilst, for customers using Darktrace with cyber analyst support services, Darktrace's Threat Intelligence Reports include observed and potential impacts to the business.

> "We previously needed three tools to tell us what Darktrace tells us on its own."
>
> BLACKHAWK NETWORK

Darktrace's Enterprise Immune System technology also facilitates companies in **"measuring the effectiveness of the cyber security controls."** As Darktrace sees and records all digital traffic, security teams can easily view whether any activity has occurred which is non-compliant with the rules and signature-based protections in place. This makes assessing the efficacy of cyber security controls simple and largely automated.

Darktrace can also provide training to SOC teams to educate on best practices and system integration of the Enterprise Immune System technology, further controls can easily **"be integrated with enterprise risk management."**

Moreover, Darktrace far exceeds the framework's requirement for **"automated real-time monitoring."** By **"continuously analyzing"** and assigning a Threat Score to all anomalous activity, Darktrace Antigena is able to take highly-targeted actions to autonomously prevent in-progress attacks. Powered by the core AI, Darktrace Antigena is an entirely unique technology that understands precisely what action to take in response to a threat to stop its spread, while failing to disrupt normal operations.

Darktrace's autonomous response solution accompanies detection tools which highlight unusual events indicative of cyber-threats, whilst also providing powerful investigation, historical data and analysis tools to an operator. Organizations which employ the Enterprise Immune System will be able to demonstrate a commitment to cyber security that goes far beyond SAMA's provisions.

About Darktrace

Darktrace is the world leader in cyber AI technology, with 7,000 deployments worldwide and over 30 offices. Founded in 2013, Darktrace has a unique combination of expertise across the fields of mathematics, software, and security intelligence. Named a finalist for the Royal Academy of Engineering's MacRobert Award and recognised as a 'Technology Pioneer' by the World Economic Forum, Darktrace's fundamental technology enables organisations to detect threats that would otherwise have gone unseen by traditional approaches and autonomously respond to developing threats in real time.

Disclaimer: This white paper is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem.