Establishment of the Financial Sector Cyber Threat Intelligence Platform (FinTIP)

Cyber-attacks can pose considerable risks to financial stability with the financial industry expected to face threats that are growing in frequency, sophistication and scope. This development is not unique to Malaysia. Globally, there has been an increasing number of cyber-attacks that have brought down key business operations. Of note, some of these were orchestrated by threat actors using highly sophisticated tactics which exploit the higher number of entry points into the network and systems of financial institutions as a result of the rapid adoption of Internet-facing systems and greater digitalisation of financial services. These threat actors operate in an active underground ecosystem where they share information, coordinate attacks, recruit hackers, sell compromised data and provide cybercrime services.

The increased intensity of such attacks and their well-coordinated nature call for a coordinated financial sector response. While financial institutions have continued to invest extensively in IT hardening and cyber resilience in their respective institutions, an industry-wide, multi-stakeholder strategy to defend the financial system against common cyber threats is needed to reinforce the efforts of individual financial institutions. To this end, the Bank has been working to establish a cyber threat intelligence and collaboration platform for the financial industry. The Financial Sector Cyber Threat Intelligence Platform, or FinTIP, commenced operations in September 2021.

FinTIP to strengthen industry collaboration and foster information sharing

The FinTIP is intended to achieve three key goals:

- Perform rapid assessment and dissemination of information on emerging cyber threats and critical IT vulnerabilities;
- Foster information sharing and collaboration across the industry via a secured and trusted platform; and
- Increase cyber situational awareness to aid strategic decision-making.

The operation of FinTIP by the Bank helps to build trust, thereby reducing a key barrier to widespread information sharing and collaboration between financial institutions and other key stakeholders. Stakeholders in public and private sectors can participate and contribute to FinTIP by confidentially sharing information on cyber threats, incidents and IT vulnerabilities in near real-time. At the national level, FinTIP serves as a bridge to connect and facilitate cross-sector information exchange between the financial sector and other economic sectors via entities such as the National Cyber Security Agency (NACSA), CyberSecurity Malaysia (CSM), Malaysian Communication and Multimedia Commission (MCMC) and Securities Commission Malaysia (SC).

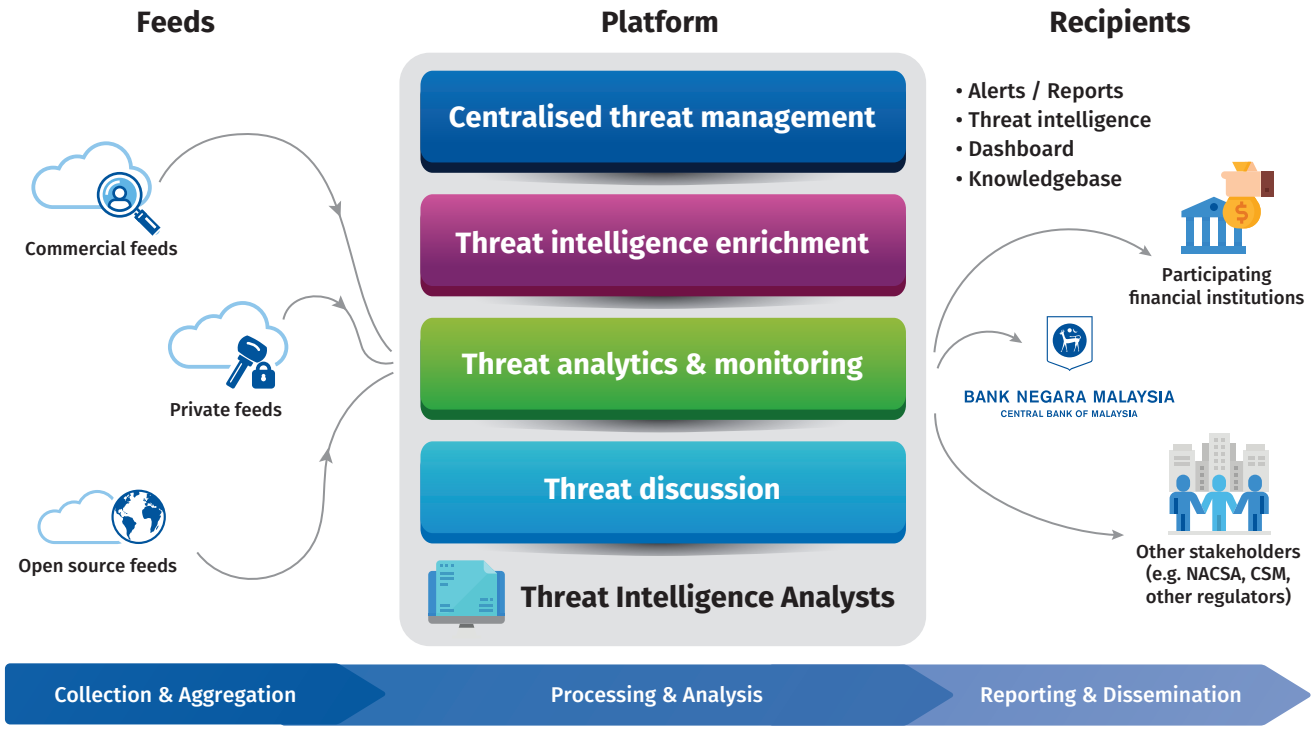
Rapid information assessment and dissemination

FinTIP, which operates on a 24x7x365 basis, will collect, aggregate and analyse cyber threat intelligence and IT vulnerabilities from various sources, and distribute relevant information to stakeholders in a timely manner (Diagram 1.3). This analytical platform leverages a combination of machine algorithms and human experts to correlate, normalise, enrich, and sanitise collected data to produce real-time actionable intelligence. Financial institutions can use the information provided by FinTIP for their own incident response, security operations, threat hunting, vulnerability management and risk analysis. They can also access professional services for assistance on cyber incident remediation and analysis of threats. Diagram 1.4 describes the key features of FinTIP.

Improving industry collaboration

FinTIP also provides a secure platform for financial institutions and other stakeholders across the industry to exchange information on defensive measures taken and lessons learnt from cyber incidents. For example, financial institutions can participate in community-driven discussions to collaborate and learn from each other's experiences in dealing with common threats. Financial institutions can also obtain an objective understanding of their cyber risk performance or exposure level, benchmarked against industry peers.

Diagram 1.3: FinTIP Deployment Model



Source: Bank Negara Malaysia

Diagram 1.4: FinTIP Features

Continuous threat landscape monitoring

Real-time dashboard – personalised dashboard consisting of representation of different data types, sightings and charts.

Exposure level – correlate submitted asset inventory against known vulnerabilities in real-time.

Peer benchmarking – measure performance or exposure level against the aggregated industry level.

Threat landscape reports – easily export periodic threat landscape report directly from FinTIP portal.

Industry broadcast & communication

Timely dissemination – of alerts and advisories to the relevant parties.

Trusted discussion channel – to facilitate information exchange and collaboration within the organisation and within the industry.

Advanced analysis by threat analysts

Malware and shellcode analysis – request in-depth analysis to understand the behaviour of potentially malicious code by submitting artefacts to FinTIP.

Sandboxing – execute untrusted programs or files via FinTIP's sandbox (safe environment).

Localised threat intelligence sharing

Secure local intelligence sharing – private intelligence feed submitted into FinTIP will be collected, sanitised and even anonymised before being shared to the wider audience.

Source: Bank Negara Malaysia

Enhancing cyber situational awareness

FinTIP increases overall industry cyber situational awareness by providing a more holistic view of threat actors targeting the local industry and helps financial institutions better understand the threat actors' tactics, techniques, and procedures. Data collected on threats and IT vulnerabilities are mapped to the IT assets used within the industry to provide an accurate localised cyber exposure level. This information will enable the Bank to pinpoint specific vulnerabilities and assess the potential system-wide impact of a cyber threat.

The reports produced by FinTIP are tactical, operational and strategic in nature to cater for a diverse audience. At the tactical level, technical reports provide granular data on cyber threat indicators which financial institutions can integrate into their cyber security tools to identify and mitigate cyber threats. At the operational level, financial institutions will be able to track attack campaigns and undertake actor profiling to gain a better understanding of the threat actors that target the financial institution. This will enable financial institutions to prioritise and perform more targeted cyber security operations. Finally, at the strategic level, financial institutions can use FinTIP data to inform business decisions by better understanding how global and local events, and the evolving threat landscape affect a financial institution's cyber security posture.

FinTIP complements existing multi-layered defence strategies

FinTIP reflects a shared responsibility for cyber security by facilitating a whole-of-industry approach towards enhancing cyber resilience. It is important to note that FinTIP serves to complement and augment, rather than replace, an individual institution's own existing cyber threat intelligence services. The Bank expects FinTIP to support deeper and faster information sharing and collaboration which in turn, will strengthen the financial industry's response capabilities to the evolving cyber threats affecting the financial system.