SKURIO

THE CYDEA TECH AND 1LINK STORY

CASE STUDY

Monitoring the Dark Web for threats to banks

Cydea Tech, an innovative cybersecurity technology provider, has implemented a managed cyber threat intelligence service for the Pakistan financial sector. The collaboration with Skurio and the industry payment technology consortium, 1LINK, gives banks vital early warning indicators of cyberattack planning and data breaches. The move follows a government directive to improve security after a 2018 incident that resulted in significant amounts of breached data appearing on the Dark Web.

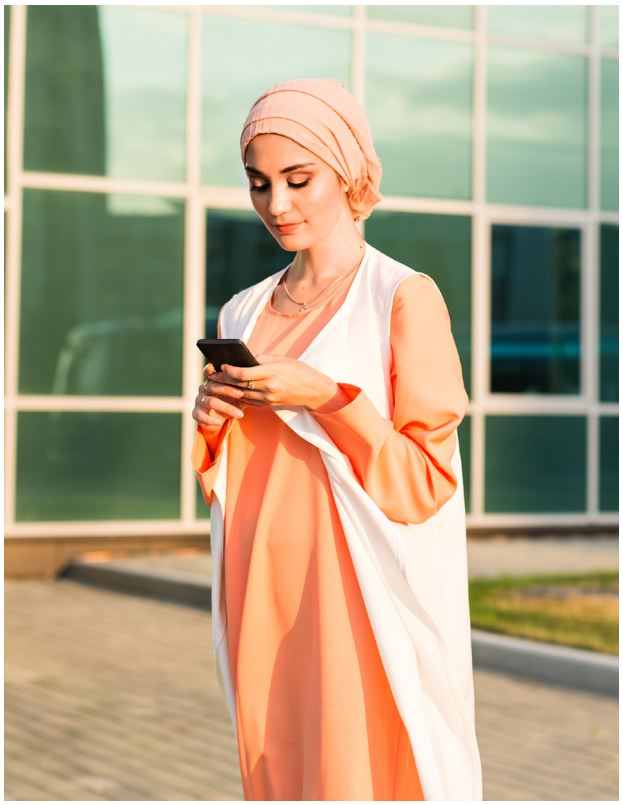
Sharing cyber intelligence amongst all financial institutions in Pakistan would be difficult without a centralised platform. Recognising the need for a trusted industry partner to be involved, Cydea Tech CEO and founder Mahir Mohsin Sheikh approached 1LINK to create a technology partnership. 1LINK works as the key switch for Pakistan's 37+ banks and financial institutions, handling a broad range of banking transactions, bill payments, fraud risk management services, and International Schemes Gateway Service. The company also launched a domestic card payment scheme, PayPak, to provide an equitable alternative for routing domestic transactions. As a result, 1LINK maintains vital experience of working with financial industry and Regulators.

PREVENTING FINANCIALLY MOTIVATED ATTACKS

For some banks, the regulatory requirement to actively share threat intelligence did not go far enough, which accelerated the need for a comprehensive Digital Risk Protection (DRP) solution. As a result, providing a Dark Web monitoring capability became a priority for Cydea Tech and 1LINK.

Eyes wide open

The prevention of financially motivated attacks is the biggest priority for banks. In October 2018, a Pakistani bank reported thefts from international payment cards. The data of various account holders had been sold on the Dark Web by hackers, and the bank was not alone in being affected. In 2009, a large amount of bank card data was put for sale on the dark web. Recently, one of the country's power generation & distribution companies, the tax collection authority, and a government-sponsored bank were also hit by cyberattacks.



Being unaware of a banking system breach and unauthorised transactions is the worst nightmare of any bank. But Digital Risk Protection helps by gathering intelligence on attack planning and breached data. This intelligence enables security teams to act quickly to mitigate the risks and reduce any associated costs of a data breach.

Faster, automated cyber threat intelligence

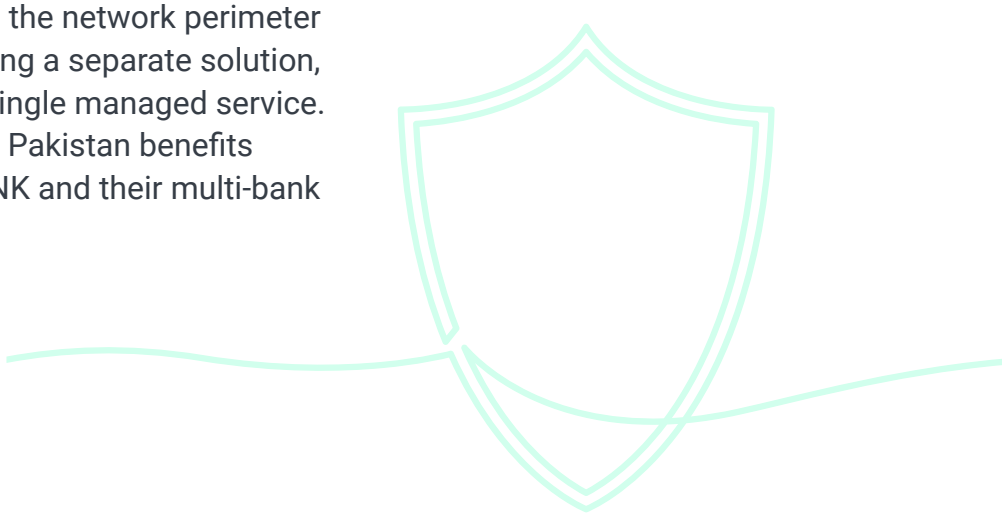
With regulatory approval for the approach, 1LINK and Cydea Tech began to prototype a solution and select a supplier for the critical DRP component. They initiated an extensive review of the DRP market to find the ideal partner and trialled several leading solutions. The Skurio analyst team proved the capability of the platform to meet the evolving use case requirements, and the solution also proved to be a superior commercial fit.

Cydea Tech intelligence analysts review threat indicators and upload them to the 1LINK Cyber Threat Intelligence Platform (1TIP). The bank's security analysts then assess how to deal with each threat and notify the banks within their framework as appropriate. The automation and sharing of cyber threat intelligence are crucial to preventing the financially motivated attacks that most banks wish to avoid.

Supporting banks with expert managed security services

Security analysts play a principal role in protecting the banking industry and bank customers. Making the best use of their time is essential, and a managed service provided by an innovative cybersecurity technology provider comes into play here. With the Skurio and Cydea Tech solution, analysts focus on processing threats and not gathering information.

Protecting data within your network perimeter is not new but actively scanning for it outside the network perimeter is. Rather than each bank developing a separate solution, Cydea Tech and 1LINK provide a single managed service. As a result, the banking industry in Pakistan benefits from economies of scale with 1LINK and their multi-bank framework.



BENEFITS OF DRP

The Skurio Advantage

Cydea Tech chose Skurio as a flexible and competitive option, and Mahir has been impressed with its ability to meet their developing needs. Skurio provides a valuable alternative to solutions that have a heavy focus on manually researched intelligence.

Pooling expertise and threat intelligence provide significant advantages. Banks across Pakistan can benefit from knowledge gained through investigations as Cydea Tech monitor local threat actor activity.

Forewarned is forearmed. With the CydeaTech service in place, banks can react as soon as a threat is detected to keep their customers' data safe and avoid data leakage. What's more, Cydea Tech will additionally focus on proactive data monitoring in the future, a capability already available with Skurio

Agility through automation

Promoting industry collaboration

Proactive threat detection

"Skurio's keyword search and monitoring make it an ideal platform for us to use for external threat hunting, it's extremely flexible."

Mahir Mohsin Sheikh Cydea Tech CEO and founder

DIGITAL RISK IN THE FINANCE SECTOR

The Bank of England's 2022 Systemic Risk survey found that **74%** of executives considered a cyberattack as their highest risk – ahead of inflation and geo-political incidents. The report cited two major factors behind the result, namely increased adoption of cloud-based services and the shift towards remote working. The banking industry is not alone in facing increased digital risk in this way. Organisations across the financial sector have seen their digital footprint expand in recent years, increasing the size of their attack surface.

Digital risk in the financial sector is a significant concern because it is a prime target for cyberattacks due to the sensitive nature of the data and financial assets it handles. From phishing scams, malware infections and denial of service attacks to data breaches, hackers seek to compromise every aspect of operations for financial gain. A successful cyberattack on a financial institution can result in the theft of sensitive customer data, financial losses, and damage to the institution's reputation.

Despite the efforts and international cooperation of crime forces, Dark Web marketplaces continue to offer stolen credit card details as well as hacked account login details for online banking and crypto accounts. In 2022, the typical cost of stolen credit card details – complete with a CVV number was as little as $20.

Financial services businesses can reduce risk by looking beyond their network for exposed data and threats. A key aspect of this is monitoring for typosquatting domains that could be used by scammers to impersonate financial brands in phishing and fraud schemes.

ABOUT US

Skurio creates innovative cybersecurity software to help you protect your organisation from digital risks. The Skurio Digital Risk Protection platform combines automated, round-the-clock monitoring of the surface, deep and Dark Web with powerful analytics capabilities for cyber threat intelligence.

hello@skurio.com www.skurio.com