SUCCESS STORY

flare

Major Canadian Bank Chooses Flare to Monitor the Criminal Underground

The customer

A client since 2018, this major Canadian bank is a leading financial institution in Canada with over $250 billion in assests.

Pain Points

Knowing the most critical threats improves reaction time and optimizes resources. The bank was looking to better understand and **prevent day-to-day cyber fraud**, gain a clearer **insight into critical threats**, and immediately mitigate and optimize the CTI team's time and resources. It had three main pain points.

Day-to-day Fraud

The CTI team needed to identify the sources of day-to-day fraud that went unnoticed for too long. Unfortunately, it was only able to build intelligence on a **limited subset of cases.** This was explained by the large number of malicious actors involved, and the small amounts stolen in each fraud. This generated too much noise for the CTI team to handle on its own.

Coverage, time, & resources

The bank's **major challenges** were trying to perform cyber-threat intelligence (CTI) activities without missing any critical information and correlating intelligence found on multiple platforms. The CTI team struggled to handle the data volume it collected from various sources, which could range in the **hundreds of thousands of web pages per week.** The CTI team was unable to link the activities of malicious actors on multiple platforms or draw an accurate picture of external threats.

Manual reporting process

Compared with other data sources such as IOC feeds, which can be directly integrated within their threat intelligence platform, the manual investigation of just a couple of websites could **use up significant resources.** The CTI team knew that monitoring events on darknet platforms was critical in getting additional actionable intelligence reporting. Even though it was already monitoring multiple websites, **keeping track of ongoing activity was challenging,** mostly because it relied on manual work. The process had to be handled while working with incident response teams, focusing on specific breaches and analyzing threats.

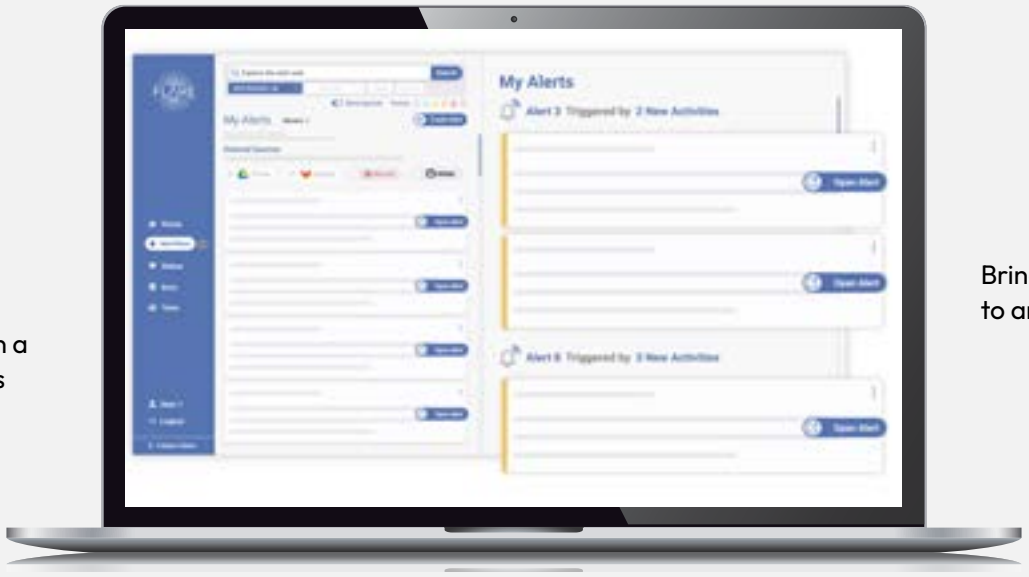
The Implementation

The bank's CTI team has implemented Firework to enhance not only **darknet monitoring** and **expand coverage through automation**, but to also gain a comprehensive view of **external threats** on both the dark and surface web. The **identifier-based alert system** delivers notifications in real-time on potential threats. The bank's CTI team also uses the platform's **search functionality** to investigate illicit markets and websites such as Github, where sensitive information can be leaked accidently without the victim ever knowing. Analysts were onboarded on Firework in a matter of hours. The adoption of **Firework required no integration.** The bank's employees were able to set up custom alerts in minutes and did not have to share any bank or customer confidential information to receive tailored alerts to monitor their digital footprint.

> Flare enables us to react quickly when threats are publicized. It helps us protect our brand and financial resournces from data breaches."
>
> -CISO of major Canadian bank

Product Highlights

Onboard and empower your existing team in a matter of hours



Bringing context to an alert helps

Higher-risk alerts are managed quickly thanks to the unique scoring system of Flare.

Impacts and Benefits

Firework has exceeded this financial institution's expectations by delivering increased productivity, an optimized reaction time, and threat landscape insights to boost security.

Reducing cyber threats to prevent day-to-day fraud

Flare **identified system vulnerabilities** exploited by malicious actors, customer accounts at risk of fraud, employee and customer credentials that may be used for **account takeover**, and any **accidental data leaks resulting from human error**. With actionable intelligence extracted from billions of data points, the CTI team optimized their time and resources to the most critical issues at hand and reduced the time to detect a security compromise from 192 days to a matter of minutes.

Enhanced coverage

Flare monitors an extensive number of illicit networks and websites on the dark and surface web that the CTI team could not cover manually on its own. With extensive **Canada-focused coverage and sources**, the CTI team now understands the local criminal underground. This enables the CTI team to stay at the forefront of all threat actors targeting its bank.

Providing intuitive insights into potential threats

The ability to pivot on data points and correlate data from all criminal underground gave the CTI team deeper insights into the threats detected. The CTI team could **track malicious actos' communication and activities across different platforms**, even when they used different usernames to hide their tracks. This provided the CTI team with an improved ranking of the most serious external threats.

Decreasing the MTTI (Mean Time to Identify) response time

The bank gained **instant visibility and 24-hour notification** of leaks and threats that jeopardized its security. The Mean Time to Identify security issues went from days to a matter of minutes. As a result of being able to see its digital footprint and external threats, the bank was able to **improve its cyber hygiene and security posture**, reducing risks.

Results

Flare's alerting system provided awareness into ongoing bank and brand-related activity on the criminal underground. This ensured peace of mind and created a safety net the CTI team could rely on to receive **instant notifications** regarding events affecting the company. The **automated process** was user-friendly and easy to handle, just as any other IOC or data feed integration. As a result of continuously monitoring its evolving digital footprint and external threats, the bank identified and remediated threats and potential data leaks in real-time, resulting in improved cyber hygiene and better security posture, which has reduced its overall cyber security risk.