SUCCESS STORY

flare

Leading Bank Responds Swiftly to Prevent Potential Major Breaches

The Customer

- Over 7 million customers in North America
- America
  Over $250B in assets
- ~50,000 employees

Challenge: Time-Consuming Manual Processes Created Inefficiencies

The security team of the major 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 security team's time and resources.

> "Thanks to Flare's intelligence, we efficiently contained a threat actor who discovered two vulnerabilities in our MFA setup. We were able to act quickly and prevent a potential serious incident."
>
> **-CISO, Leading Bank**

Day-to-Day Fraud

The security team needed to identify sources of day-to-day fraud that went unnoticed for too long. Unfortunately, they were only able to build intelligence on a limited subset of cases. A large number of threat actors stole small amounts in each fraud, which generated too much noise for the security team to handle on their own.

Coverage, Time, and Resources

The security team wanted to perform CTI activities without missing any critical information and correlating intelligence found on multiple platforms. The security 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 security team was also 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 security team knew that monitoring events on dark web 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 security team sought out Flare to:

- Enhance dark web monitoring, and expand its coverage through automation
- Gain a comprehensive view of external threats on both the clear & dark web

Benefit: React Faster than Ever Before to External Threats

> "Flare enables us to react quickly when threats are publicized. It helps us protect our brand and financial resources from data breaches."
>
> — CISO, Leading Bank

Analysts onboarded onto Flare in a few hours, and the adoption required no integration. They were able to set up custom alerts in minutes and didn't have to share any internal or confidential information from customers to receive prioritized actionable alerts to monitor their external threats. The identifier-based alert system delivers notifications in real-time on potential threats.

Below are the ways the security team enhanced their capabilities with Flare.

Reduce Cyber Threats to Prevent Day-to-Day Fraud

Flare identifies:

- System vulnerabilities exploited by threat actors
- Customer accounts at risk of fraud
- Employee and customer credentials that may be used for account takeover
- Accidental data leaks resulting from human error

With actionable intelligence analyzed from billions of data points, the CTI team optimizes their resources to the most critical issues, reducing the time to detect a security compromise from days to minutes.

Increase Coverage, Include Relevant Location-Specific Sources

Flare monitors an extensive number of illicit forums and markets on the clear & dark web and Telegram. The security team could not cover this manually on their own. With extensive coverage of certain location-based sources, the security team understands the local criminal underground well.

Provide Insights into Potential Threats

The ability to correlate data from all cybercrime sources gives the security team deeper insights into the detected threats. The CTI team could track malicious actors' communication and activities across different platforms, even when they used different usernames to hide their actions. This provides the security team with an improved prioritization process of the most critical external risks.

Decrease Mean Time to Identify (MTTI) Response Time

The security team gained instant visibility and 24 hour notifications of threats. The mean time to identify security issues plummeted from days to minutes.

Preventing a Possibly Costly Breach from a Exploited Bug

- When a threat actor published an ad selling a method to bypass the security questions used to validate a client's identity when logging in to the online banking platform, Flare alerted the security team immediately.
- The security team identified and fixed the vulnerability exploited by the threat actor to gain access to customers' accounts.
- Three days later, the same threat actor posted an updated ad with a new working method.
- Flare once again alerted the security team, which launched a second round of review to identify and fix the new bug.
- Afterwards, the threat actor removed the ad, and the security team confirmed they fixed the bug.
- Through actionable intelligence with Flare, security teams stay ahead of threats, react quickly, and protect their assets better.

Flare enables the security team to be aware of ongoing activities concerning them in illicit communities, establishing a safety net that the security team could rely on for relevant instant notifications. This ensures peace of mind. This automated process is user-friendly. As a result of automated continuous monitoring of its external threats, the security team identifies and remediates (potential) threats in real time, resulting in boosting their security posture and slashing overall cyber risk.