SUCCESS STORY

Large North American Bank Streamlines Sensitive Leaks Monitoring, Significantly Cutting Incident Response Costs

The Customer

- One of Canada's largest financial institutions
- Close to **50,000 employees**
- **Hundreds of billions** in assets

The Challenges

Increasing Surfaces to Monitor Online

The CTI team knew they should be monitoring GitHub and other shared repositories, but among all the other sources, it was often skipped due to the content's complexity. Periodically, a CTI analyst would manually run searches on GitHub based on the high level queries. The number of results was overwhelming and identifying potential leaks took enormous time investment.

Multiple data leaks were still found during that period, either by the CTI analysts themselves or by their peers on other teams. The findings led to full-blown incident response operations, generally involving a task force of six people. These included analysts, managers, and directors assembled in a war room for six to seven hours trying to make sense of the data leak. They had to:

- Find its source
- Identify potential impacts
- Rotate credentials and API keys
- Contact a number of additional current and former employees

The bank's CISO was also personally involved every time, as the threat level was always unknown at the beginning of the incident.

The Implementation

The CTI team tested multiple monitoring solutions to improve their monitoring and response capabilities, but the level of noise and false positives made many tools an additional burden for the team. Flare was the only solution among the lot that was able to combine state of the art data collection systems with a noise reduction and prioritization engine that gave them the necessary context to be able to classify each data leaks' criticality level without hundreds of hours of work.

The bank's CTI team was onboarded in a few hours. They used their newfound bandwidth to optimize downstream processes of incident response.

The CTI team built a powerful process around the platform and its scoring system. Higher-risk alerts are managed quickly by the team, and clear guidelines have been put in place for different types of data leaks. Managers and employees are quickly alerted to the situation and informed of remediation actions that must be taken.

> **Whereas other solutions would present us with thousands of potential leaks which were impossible to work with for our small team, Flare was the only one that could successfully filter and prioritize data leaks with their 5-point scoring system.**
>
> -CTI Director
>
> Major North American Bank

Impacts and Benefits

Cost Effectiveness

With the combination of the platform and the newly built processes, the CTI tam was able to operationalize and proactively respond to technical data leaks. No war room is required, and the CISO can be informed in weekly briefings of any remediation actions that took place, and does not have to be actively involved unless the leak is immediately classified as very high risk.

More Detection, Better Protection

Today, the bank's cyber threat team works hand in hand with Flare to target harder to detect, complex data leaks that would be difficult to find even for domain experts. Flare enables the bank to remediate issues such as an API key being leaked in a code file where the organization's domain name is not even present. Some of these have been integrated into Flare, increasing the number of findings while reducing unnecessary noise.

Handling an Incident

In a recent case, Flare detected sensitive data that had been posted by a previous employee. The CTI team promptly identified and notified the ex-employee's superior, who contacted the individual in question and asked for the content to be removed. Less than 30 minutes after the Flare alert, the content was removed from GitHub and the incident was contained.