SUCCESS STORY

flare

Major Bank Streamlines Technical Leaks Monitoring and Significantly Cuts Incident Response Costs

The Customer

- Close to 50,000 employees
- Hundreds of billions in assets

Employee errors can lead to leaked credentials, API keys, personally identifiable information (PII), and intellectual property. While there is no malicious intent behind these risks, they can cause just as much damage as a cyberattack and require active mitigation efforts.

When private repositories are accidentally made public, or threat actors infiltrate repositories that should be restricted, threat actors can steal sensitive information such as login credentials, certificates, and API keys on the clear web

> "When a previous employee posted sensitive information, with Flare's alert we sprang into action and contained the incident in 30 minutes."
>
> **-CTI Director, Major Bank**

The number of different data sources to simultaneously monitor and the rapidity at which new data is posted online poses an enormous challenge to resource-constrained security teams. In addition, the reliability of data collection and monitoring, as well as the accuracy of the internal alerting system, is key to effective risk management.

The raw data needs to be contextualized to be able to rapidly assess how critical it is. Noise reduction is key since the amount of information collected makes mere collection and aggregation insufficient.

The security team of a major bank struggled to effectively and consistently monitor clear web leaks from human error such as from GitHub. When the security team did find leaks, this would cause a war room response that took hours to resolve because of the lack of visibility into the leak.

Challenge: Increasing Clear Web Surfaces to Monitor

The security team of a leading bank knew they should be closely monitoring GitHub and other shared repositories, but it was often skipped due to the content's complexity. Periodically, a security 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.

Security analysts or their peers on other teams found multiple data leaks, which would lead to full-blown incident response operations. Generally, this involved a task force of six people including analysts, managers, and directors assembled in a war room for six to seven hours trying to make sense of the data leak by:

- Finding its source
- Identifying potential impacts
- Rotating credentials and API keys
- Contacting additional current and former employees

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

Implementation: Flare Cuts Out Noise Unlike Other Solutions

The security team tested multiple 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 that combined state-of-the-art data collection systems with robust noise reduction and prioritized alerts that gave them the necessary context to instantly be able to classify each data leak's criticality level without hundreds of hours of work.

The security team was onboarded in a few hours and took advantage of their newfound bandwidth to optimize downstream processes of incident response.

> "Other solutions would present us with thousands of potential leaks which were impossible to work with. Flare was the only one that could successfully filter and prioritize data leaks."
>
> — CISO, Leading Bank

Benefit: Significantly Cut Incident Response Costs

With the combination of Flare and newly built processes, the CTI team now operationalizes and proactively responds to technical data leaks. There's no more war room required, and the CISO is 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.

Handling an Incident in 30 Minutes with Flare

Flare detected sensitive data that had been posted by a previous employee. The security team promptly identified and notified the former employee's manager, who contacted the individual in question, asking to remove the content. Less than 30 minutes after the Flare alert, the sensitive information was removed from GitHub and the security team contained the incident.

Flare enables the bank to target harder to detect, complex data leaks that would be difficult to find even for domain experts (for example, an API key leak in a code file in which the organization's domain name isn't present). This increases the number of findings while reducing unnecessary noise.