sixgill

CASE STUDY

# Financial services: Revolutionize SOC threat intelligence

## CLIENT PROFILE

A financial services multinational with over 5,000 employees and more than 2500 branches spread over 20 countries. The client has a global Security Operation Center (SOC) and Computer Security Incident Response (CSIRT) teams in several key locations.

## EXECUTIVE SUMMARY

The client's SOC was facing severe challenges by relying on manual intelligence feeds: it was either irrelevant (dated), or inaccurate (loaded with false-positives). This created gaps and bottlenecks, with analysts collapsing under the volume of manual work required to produce quality intelligence.

As part of an effort to accelerate time-to-intel and optimize work flows, the company chose Sixgill Darkfeed. Initially embraced by CSIRT, teams integrated the Darkfeed intelligence stream into their security stack and began to see clear and instant value. Later, usage was expanded to additional threat intelligence teams who began using Sixgill's investigative portal, and the value grew exponentially.

## CHALLENGE

- Dated, irrelevant and inaccurate threat intelligence, hindering their ability to perform optimally
- Constant information fatigue due to data overload
- Lack of context and visibility into an attacker mindset

> **“Darkfeed has exceeded all our projections: It's like having tomorrow's newspaper in hand today.”**
>
> *CISO*

## SOLUTION

With Darkfeed, the CSIRT teams' daily responsibilities changed dramatically:

- Preemptively identify and block threats
- Substantially reduce false-positives
- Maximize security systems' effectiveness
- Understand the full picture behind malicious threat vectors
- Dramatically reduce response time and number of attacks

## CISO SELECTS DARKFEED TO TRANSFORM ITS THREAT INTELLIGENCE

- Accelerate data extraction - 24x faster
- Increase detection of threats - 7x detection
- Increase response time - 4x faster

## CHALLENGES

With the cyber threatscape growing at an alarming rate, the SOC's threat intelligence and CSIRT teams had to rely only on two threat intelligence feeds: manual feed, containing week-old information, and telemetry, which was loaded with false-positives. That meant that information was either irrelevant (too old), or inaccurate (loaded with false-positives). The volume of data that needed to be scanned in order to extract relevant intel was growing rapidly, creating intelligence bottlenecks and "information fatigue" - a term coined by analysts collapsing under the volume of manual work required to create quality intelligence. As part of an effort to accelerate time-to-intel and optimize workflows, the company chose Darkfeed.

> **"I've never seen such results: it totally reduced alert fatigue, providing me with the full picture behind each and every indicator of threat. With Sixgill, we've been able to preempt a large number of attacks and improve our response time significantly."**
>
> *Threat analyst*

## HOW DARKFEED HAS HELPED

Initially adopted by IR teams, Darkfeed seamlessly integrated to the client's SIEM, SOAR, and VM platforms as well as their Firewall. The IR teams saw instant value. By having preemptive, fresh intelligence (within hours instead of days), they were able to instantly reduce response time by 75% and detect 7x more threats. Realizing the value, the threat intelligence team expanded the service to include Sixgill's investigative portal with actionable alerts. This allowed them to further investigate IOCs in real-time and keep the threatscape updated with all the details, from time of exposure to time of investigation. The portal thereby accelerated detection and remediation while providing unmatched visibility and insight into each and every threat actor's context, history and mindset.

## THE RESULT

**4x**
Faster response

**24x**
Faster data extraction

**4x**
Detection of threats

The client's security teams continue harnessing the cumulative powers of Sixgill's Darkfeed and investigative portal to expand the use cases of integrated threat intelligence, maximizing its performance.