CASE STUDY

Financial Services

Cybersixgill's intelligence feed reduces incident response times by 75%

At a glance

- Europe
- $25million+
- 5,000+ employees
- Financial Services

Overall benefit

Early indications of risk transformed a bank's security posture from reactive to proactive

The Challenge

A financial services multinational with over 5,000 employees and more than 2,500 branches spread over 20 countries was facing severe challenges. 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.

The intelligence the team gathered was either irrelevant (too old), or inaccurate (loaded with false-positives). In addition, the volume of data that needed to be scanned in order to extract relevant intel was growing rapidly, creating intelligence bottlenecks and information fatigue. This resulted in a reactive security posture and a team that lacked context and visibility into the attacker's mindset, placing the organization at risk.

The Solution

As part of an effort to accelerate time-to-intel and optimize work-flows, the company chose Cybersixgill's threat intelligence with indicators of compromise (IOC) module. Initially adopted by IR teams, the IOC feed was seamlessly integrated to the client's SIEM, SOAR and VM platforms as well as their Firewall.

Later, usage was expanded to additional threat intelligence teams who began using the Investigative Portal, and the value grew exponentially. Fraud teams are now able to accelerate the discovery and remediation of zero-day exploits and threats, prioritizing their responses to malicious activity across various units in the enterprise. They now also have access to unprecedented actionable fraud related intelligence in real-time, receiving customized fraud notifications to assist remediation efforts. "With Cybersixgill, we've been able to preemptively detect and block credit card fraud," comments the firm's Senior Fraud Analyst.

The Results

The IR teams saw instant value. By having preemptive, fresh intelligence (within hours instead of days), they were able to instantly reduce response times by 75% and detect 7x more threats.

> “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 Cybersixgill, we’ve been able to preempt a large number of attacks and improve our response time significantly.
>
> **Threat Analyst**

Realizing the value, the threat intelligence team expanded the service to include the Investigative Portal with actionable alerts. This empowered them to further investigate IOCs in real-time. The Portal accelerated detection and remediation times, while providing unmatched visibility and insight into each and every threat actor’s context, history and mindset. “It has exceeded all our projections: It’s like having tomorrow’s newspaper in hand today,” commented the firm’s CISO.

About Our Threat Intelligence Feeds

Combining unparalleled threat data collection capabilities with limitless search functionality and automation, Cybersixgill threat intelligence delivers contextual visibility into the clear, deep and dark web. Our API integration provides secure access to our complete body of collected intelligence, integrating seamlessly into your workflows and system architectures. Proactively prioritize and respond to threats that are targeting your critical assets, prevent fraud, data breaches and investigate threats in real-time to minimize your attack surface.

Learn more about our threat Intelligence API feed and how it can support your ongoing cyber security activities.

Explore the Investigative Portal >

Explore Darkfeed >

cybersixgill

Book a Demo

Visit Cybersixgill

Follow us