cybersixgill

CASE STUDY

Darkfeed supercharges Cortex XSOAR accelerating time-to-intel

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

A multinational financial services client was facing several challenges, mainly relating to cyber and fraud. By relying on manual intelligence that was either irrelevant (dated), or inaccurate (loaded with false-positives), they faced many gaps and bottlenecks, with analysts collapsing under the volume of repetitive manual work required to produce quality intelligence.

In addition to the Cortex XSOAR integration, the security team chose Sixgill for automation of data enrichment and threat intelligence management in an effort to accelerate time-to-intel, improve intelligence relevancy, and optimize strategy. Time-to-value was instant. The intuitive interface and the ability to gain instant visibility into a threat actor's mindset, history and context quickly led to an exponential expansion of use. Security teams now leverage Sixgill to extend the use cases for fraud-related threats, maximizing Cortex XSOAR effectiveness.

CHALLENGE

- Dated, irrelevant and inaccurate threat intelligence, hindering their ability to perform optimally
- Continuous alert fatigue due to data overload
- Lack of fraud related real-time intelligence alerts

SOLUTION

With Cybersixgill, security and fraud teams could finally:

- Accurately prioritize responses and suggest remediation steps across various units in the enterprise
- Understand the full picture behind malicious threat vectors in real-time
- Accelerate discovery and remediation of zero-day exploits and threats
- Gain unprecedented actionable insight to customized fraud related intel in real-time

> **"Not only did Cybersixgill provide our fraud teams with real-time intelligence, it has transformed our ability to understand and minimize digital risk across the entire organization"**
>
> *CISO*

CYBERSIXGILL SUPERCHARGES THREAT INTELLIGENCE

- Accelerate data extraction - 24x faster
- Increase detection of leaked creditcards - 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 manual feeds, containing week-old information and telemetry, which was loaded with false-positives. That meant that information was either irrelevant or inaccurate. The volume of data that needed to be scanned in order to extract relevant intel and amount of repetitive work was growing rapidly, creating intelligence bottlenecks. Fraud teams suffered a similar situation, with analysts collapsing under the volume of manual work required to create quality intelligence while producing insuficient results. As part of an effort to accelerate time-to-intel and optimize workflows, the company chose to integrate Cortex XSOAR with Cybersixgill.

> "I've never seen such results: it totally amplifed the value we get from XSOAR. With Cybersixgill, we've been able to preemptively detect and block credit card frauds - right from XSOAR's dashboard."
>
> *Senior fraud analyst*

HOW CYBERSIXGILL HELPED

Cybersixgill's Darkfeed seamlessly integrated with the client's SOAR system (Cortex XSOAR), pushing deep and dark web based IOCs with actionable insights. Security teams saw instant value by reducing response time by 75%. Realizing that, fraud teams, with the help of Cybersixgill's CSM team, expanded the service to the Cybersixgill Investigative Portal in order to deepen real-time investigation and receive customized fraud notifications. With this powerful combination, fraud teams got alerts about leaked credit cards the moment they surfaced on the deep and dark web. They were able to use AI-based automatic analytics for root-cause analysis and get ultra-deep reports, enriched with context and metrics like never before. With the portal and Darkfeed working together, they were able to further block and investigate IOCs in real-time and keep the threatscape updated. From domain squatting and phishing attacks to leaked credentials or cards. Using Cortex XSOAR with the Cybersixgill portal and Darkfeed provided unmatched visibility and insight into each and every threat actor's context, history and mindset - elevating both Cortex XSOAR and the team's performance and value.

THE RESULT

24x
Faster data extraction

7x
Detection of credit cards

4x
Faster response

The client's fraud and security teams continue to harness the combined powers of XSOAR and Cybersixgill to expand the use cases of integrated threat intelligence and maximize its performance.