cybersixgill

snowflake

Snowflake & Cybersixgill - Threat Intelligence at Cloud Scale

Together, Snowflake & Cybersixgill bring scalability, speed and automation to cybersecurity - providing customers with seamless access to best-in-class threat intelligence in a unified, cloud-native security data lake.

Snowflake's Security Data Lake

To keep pace with the demands of today's cloud workloads and reduce the operational limitations on security teams, Snowflake has expanded their cloud-native data management solution to security analytics, bringing big data to cybersecurity in a holistic security data lake. By bridging the divide between internal enterprise data and security data sourced from external vendors, Snowflake's security data lake architecture democratizes the security stack to support specialized cybersecurity solutions. As in all modern cybersecurity and risk management programs, within this modern security data lake, threat intelligence is the fundamental fuel, delivering critical information and data about cyberthreats and the capabilities, opportunities and intent of the adversaries behind them.

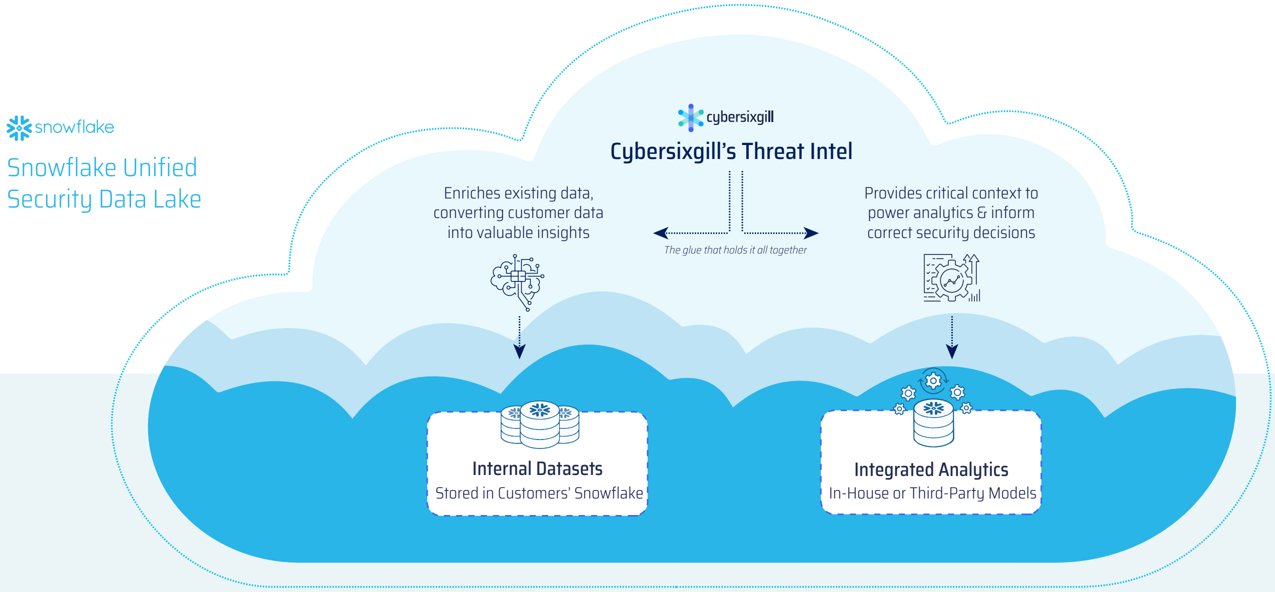
Cybersixgill's Cyber Threat Intelligence

Over the past few years, Cyber Threat Intelligence (CTI) has been embraced as a core component of cybersecurity service offerings, recognized as a powerful and cost-effective tool to improve the productivity of security operations and facilitate a proactive approach to building organizational cyber resilience. Threat Intelligence helps organizations understand & prepare for their own unique threat landscape, enhance overall risk posture, and improve other operational efforts such as incident response, threat hunting & vulnerability management. Yet, while cyberthreats continuously evolve and develop, many of the predominant threat intelligence methodologies remain rooted in the approaches of yesterday, confined by siloed teams, manual processes, outdated information, limited understanding of cyberthreats and threat actors, and slow responses. With the maturity of machine learning, NLP, and big data, Cybersixgill has made great strides in the threat intelligence evolution, transforming current processes to meet the demands of the modern threat landscape. By automating the production cycle of threat intelligence, Cybersixgill brings agility to the cyber chain of command, empowering teams to identify, analyze, correlate and respond to threats in real-time while proactively disrupting future attacks.

With this strategic partnership, Snowflake users can seamlessly integrate Cybersixgill's industry-leading real-time cyber threat intelligence data through the Snowflake Data Marketplace, and gain full visibility into their organizational threat landscape at massive scale.

In a single, unified data layer within the customer's Snowflake, users can enrich their internal organizational datasets with Cybersixgill's real-time threat intelligence data, and deploy custom analytics at cloud scale. This allows Snowflake customers to streamline the threat hunting process, accelerate incident prevention and response, create automations to block malicious IOCs in real-time, drive internal security applications and establish in-house threat detections and risk scores based on first-round integrated threat intel insights - boosting their cyber resilience to meet the demands of the current threat landscape.

CTI - The Glue Holding the New Security Stack Together



snowflake

Snowflake Unified Security Data Lake

cybersixgill

Cybersixgill's Threat Intel

Enriches existing data, converting customer data into valuable insights

Provides critical context to power analytics & inform correct security decisions

The glue that holds it all together

Internal Datasets
Stored in Customers' Snowflake

Integrated Analytics
In-House or Third-Party Models

Cybersixgill's Benefits:

Cybersixgill's CTI solutions are powered by the most extensive, automated collection of threat intelligence from the cybercriminal underground, providing exclusive and real- time access to the largest database of deep, dark and clear web activity on the market. Our proprietary algorithms extract data from a wide range of sources, including content from limited-access deep and dark web forums, underground markets, invite-only messaging groups on Telegram, Discord and QQ, as well as an unparalleled archive of indexed, searchable historical data from as early as the 1990s. This data is then enriched with machine learning techniques to create profiles and patterns of malicious threat actors and their interactions with peers across platforms, which otherwise remain invisible or inaccessible to enterprises.

Consume cyber threat intel directly from your Snowflake Datalake to drive informed security decisions.

Combine real-time threat intel with internal datasets in a centralized platform for full visibility into your threat landscape.

Integrate SIEM capabilities at cloud scale, powered by the most extensive feed of CTI from the deep & dark web.

Gain critical insights into malware-related TTPs & trends to block emerging threats before they are deployed in the wild.

Personalized Threat Intelligence Listings

Complete Darkfeed

Darkfeed is the most comprehensive stream of malicious Indicators of Compromise (IPs, URLs, malware hashes, RDPs, and more) on the market - autonomously extracted and delivered in real-time. While most TI feeds are generated from telemetry - detecting attacks already in progress - Darkfeed collects, tags and filters IOCs sourced directly from chatter among cybercriminals in the underground, capturing emerging threats in the earliest stages of the malicious supply chain as they surface on the forums and markets of the deep & dark web. Darkfeed's indicators are both unique (66% undetected by other antivirus vendors), and proactive, alerting to an IOC days or even months before it is weaponized in an attack and detected by traditional telemetry.

Coming Soon

Threat Hunting Package | Vulnerability & Exploit Package | Incident Response Package | Fraud Package

Standard Listings

Cybersixgill also offers three free data subset listings from our vast collection of threat intelligence from the cybercriminal underground, segmented according to use case:

Malware-Related Intel & Insights from the Deep & Dark Web:

Automate IOC blacklisting and gain insight into malware-related TTPs to preemptively block items that threaten your organization.

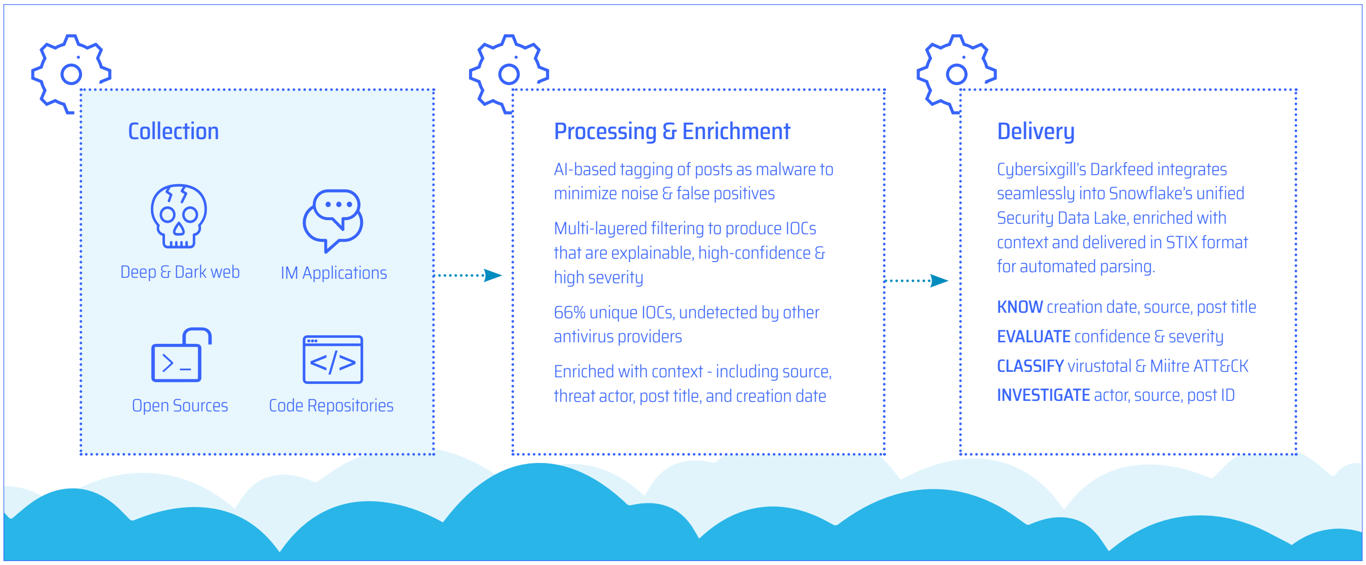
Compromised Sites Mentioned on the Deep & Dark Web:

Establish automated remediation processes against phishing campaigns and ransomware attacks using malicious domains & URLS.

Compromised End-Points & Access Mentioned on the Deep & Dark Web:

Protect your network from initial access brokers and ransomware deployment by way of compromised RDP, FTP and VPS connections.

Under the Hood: Darkfeed & Snowflake



Processing & Enrichment

AI-based tagging of posts as malware to minimize noise & false positives

Multi-layered filtering to produce IOCs that are explainable, high-confidence & high severity

66% unique IOCs, undetected by other antivirus providers

Enriched with context - including source, threat actor, post title, and creation date

Delivery

Cybersixgill's Darkfeed integrates seamlessly into Snowflake's unified Security Data Lake, enriched with context and delivered in STIX format for automated parsing.

KNOW creation date, source, post title

EVALUATE confidence & severity

CLASSIFY virustotal & Miitre ATT&CK

INVESTIGATE actor, source, post ID

Cybersixgill brings agility to cyber defense, with fully autonomous threat intelligence solutions to help organizations proactively detect and protect against phishing, data leaks, fraud, malware and vulnerability exploitation - enhancing cyber resilience and minimizing risk exposure in real-time. The Investigative Portal provides covert access to threat intel from the deep and dark web, complete with context and actionable insights for remediation. Seamlessly integrated into existing security systems, DarkfeedTM enriches endpoint protection by preemptively blocking malicious IOCs, while CVE insights from the DVE ScoreTM transform vulnerability management, predicting the immediate risk of vulnerability exploitation based on threat actor intent. Current customers include global enterprises, financial services, MSSPs, government and law enforcement entities.

Learn more at cybersixgill.com

Snowflake Cloud Data Platform shatters the barriers that prevent organizations from unleashing the true value from their data. Thousands of customers deploy Snowflake to advance their businesses beyond what was once possible by deriving all the insights from all their data by all their business users. Snowflake equips organizations with a single, integrated platform that offers the only data warehouse built for any cloud; instant, secure, and governed access to their entire network of data; and a core architecture to enable many other types of data workloads, including a single platform for developing modern data applications. Snowflake: Data without limits.

Find out more at snowflake.com