cybersixgill

AUTONOMOUS CYBER THREAT INTELLIGENCE

KNOW WHAT'S OUT THERE

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 & dark web forums, illicit underground markets, invite-only messaging groups, code repositories and paste sites, as well as an 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 peer networks across platforms, to provide a complete, context intelligence picture.

Cybersixgill's threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, equipping security teams with the insights they need to protect their various assets in the face of the ever-accelerating cyber threat landscape.

Quantifiable benefits of up to 311% ROI on security investment

Maximize performance of analysts, platforms & processes by up to 5x

Easily scale SecOps with automatic extraction, analysis & prioritization

Increase analysts' efficiency and productivity to meet growing demand

Why Cybersixgill?

Other vendors	Cybersixgill
☹ Collect data using obsolete, manual approaches that rely on humans to search for and extract intelligence and fail to continuously detect threats.	☺ Fully automated, real-time intelligence collection, extraction and indexing - promising more data, less blindspots and greater value generation for customers.
☹ Manually curated reports and feeds which do not provide the full intelligence picture regarding the nature and source of each threat, forcing clients to make critical decisions with little information.	☺ Provides complete and unrestricted access to our complete body of contextual threat intelligence, empowering customers to conduct their own independent investigations and regain control of their cybersecurity program.
☹ Significant lag-time between detection and alert, by which time the threat has likely been weaponized and the incident may have already occurred.	☺ Provides actionable and relevant threat alerts in real-time, minutes after it has surfaced on the underground, along with actionable recommendations for remediation.
☹ Limited scalability and complex pricing packages, with meagre quantifiable ROI.	☺ Maximizes analysts' performance, eliminating staff expansion while supporting new service offerings, with a quantified ROI of up to 311%.
☹ Limited integration with modern security products and architectures.	☺ Tech-agnostic and seamlessly integrated into customers' existing security stack.