cybersixgill
A BITSIGHT Company

INVESTIGATIVE PORTAL

A SINGLE SOURCE OF TRUTH FOR CLEAR, DEEP AND DARK WEB CYBER THREAT INTELLIGENCE

Lower the learning curve for threat intelligence analysts with direct access to critical deep & dark web intel in a single, searchable investigative platform. Embedded with Cybersixgill IQ, the Investigative Portal harnesses cutting-edge generative AI to transform vast volumes of CTI data into easily accessible and actionable insights, enabling customers to reduce employee hours by more than 85% in the first year of implementation.

Monitor Emerging Cyber Risks In Real-Time

By combining continuous collection capabilities with search functionality, security automation and AI, the Investigative Portal delivers unmatched contextual visibility into the underground threat landscape.

In a single, centralized SaaS dashboard, analysts gain unrestricted access to Cybersixgill's complete body of collected threat intel, including billions of intelligence items from the deep, dark and clear web.

Each item is enriched with critical context and valuable insight into the nature, source, relevance and urgency of each threat. Combining these features with custom alerting and monitoring, Cybersixgill's Investigative Portal dramatically enhances the productivity and efficiency of security teams.

When compared to our closest competitor, Cybersixgill delivers:

+10m
NEW INTEL ITEMS INDEXED PER DAY

10x
COLLECTION FROM DARK WEB SOURCES

24x
FASTER DATA EXTRACTION

Continuously Exposing The Earliest Indications Of Risk

Uncover threat actor activity in any language, format and platform with exclusive, simplified, real-time access to the largest database of deep, dark and clear web activity on the market. Our proprietary algorithms infiltrate and extract data from the most extensive base of sources, including:

- Limited-access deep & dark web platforms
- Invite-only messaging groups
- Paste sites
- 7 million+ threat actor profiles
- High-value sites with complex CAPCHA
- Underground markets
- Code repositories
- Clear web platforms
- Social media
- Archive of historical data from as early as the 1990s
- Deleted posts

Features:

The Cybersixgill Investigative Portal provides a safe and searchable conduit for deep, dark and clear web cyber threat intelligence investigation and analysis.

- Interactive threat intel experience with conversational AI chat interface
- Simplify complex intelligence with ai-generated summarizations and insights
- On-demand AI-powered intelligence generation, tailored to industry, persona, geography and business needs
- Collaborative case management & slack-like chat feature
- Trending cyber news
- Customized reports & RFIs
- Automated alerts triggered by organizational assets
- Flexible multi-tenancy support for MSSPs
- Vulnerability & Exploit intelligence module* (sold separately)
- Integrated mapping to the MITRE ATT&CK framework
- Detailed analysis of malware strains

Preempt threats and accelerate your mean time to detect

✓ Cybersixgill captures, processes and prioritizes emerging threats, TTPs and IOCs in real-time, moments after they surface on the clear, deep and dark web.

✓ Multi-layered filtering and tagging processes to eliminate false-positives and ensure data fidelity.

✓ Cybersixgill IQ makes threat intelligence accessible at all levels of expertise, transforming complex raw intelligence into simplified human-readable insights.

Expose risks as they emerge:

- Fully automated collection and source-infiltration, with ability to scrape data inaccessible to other vendors.
- Processes data in all languages and formats, with autonomous translation and image-to-text content extraction.
- Advanced AI & ML index, correlate, analyze, tag and filter raw data, enriching each item with rich context to derive critical intelligence regarding the nature, source and evolution of each threat.
- Comprehensive threat actor profiles, detailing their languages, history, arenas of activity, TTPs, interests, peer networks & interactions and more.

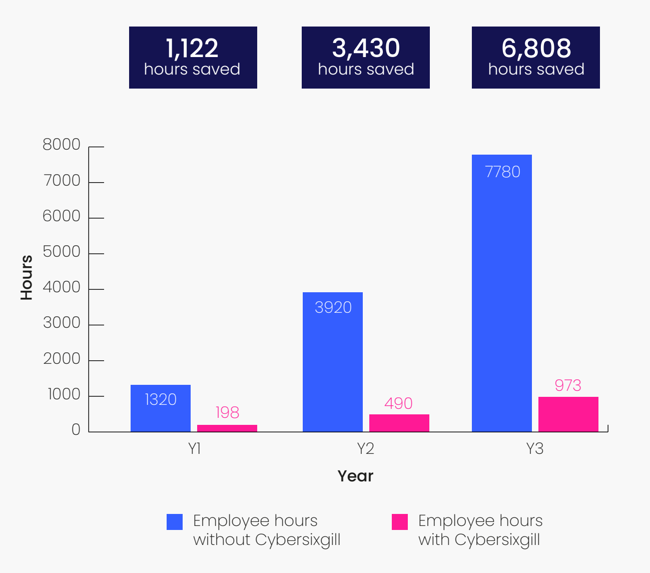
> “Cybersixgill helped us track and gain insight into Dark & Deep web intelligence. The coverage is incredible; compared to other vendors we used and tried, they have the best snapshot of dark & deep web forums, chats, and markets”
>
> Accenture

Streamline through integrations into existing systems and workflows

- Easy to use interface for seamless onboarding and instant time-to-value.
- Easily customize alerts and notifications based on your defined organizational assets (Aliases, Domain Names, IP Address, Executives, Products & Services, Third Parties, Exposed CVEs, BINs, and more).
- Each organizationally-specific alert is presented with critical contextual insight into the nature of the incident (date, description, triggered asset), the source of the incident (actor, site, post details, peer interactions, and more), a classification of the threat type (i.e. fraud, compromised account, etc.), the urgency of the threat (imminent / emerging), status (treatment required, in treatment or resolved), and actionable assessments and recommendations for remediation.
- Native, multi-tenant, role-based architecture and case management for MDR and MSSPs supporting total data separation in a single deployment.

Accelerate & Enhance Productivity

Reduce staff labor efforts and avoid staff expansion while meeting growing threat intelligence business demands.



Why Cybersixgill Is Different

Cybersixgill	Other Vendors
AI is only as valuable as the data it is trained upon. Cybersixgill's IQ is trained upon our market-leading CTI data from the deep, dark and clear web, transforming the threat intelligence experience across the entire solution	Rudimentiary AI integration, not trained on threat intelligence data, limited to translating human-language queries into search syntax
Fully automated, real-time intelligence collection, extraction and indexing - promising more data, less blindspots and greater value generation for customers.	Collect data using obsolete, manual approaches that rely on humans to search for and extract intelligence and fail to continuously detect threats.
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.	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 actionable and relevant threat alerts in real-time, minutes after it has surfaced on the underground, along with actionable recommendations for remediation.	Significant lag-time between detection and alert, by which time the threat has likely been weaponized and the incident may have already occurred.
Maximizes analysts' performance, eliminating staff expansion while supporting new service offerings, with a quantified ROI of up to 311%.	Limited scalability and complex pricing packages, with meager quantifiable ROI.
Tech-agnostic and seamlessly integrated into customers' existing security stack.	Limited integration with modern security products and architectures.