sixgill

PORTAL BY SIXGILL

Empowering security teams with a premium threat intelligence investigation portal and the most comprehensive data sources out there

AUTOMATED | ACTIONABLE | COMPREHENSIVE | REAL-TIME

Sixgill is an enterprise-grade, leading SaaS threat intelligence provider that helps enterprises, MSSPs, financial services leaders, government and law enforcement entities, to fight cyber crime through its deep and dark web threat intelligence solutions.

Sixgill is the only solution that is comprehensive, covert and fully automated. It empowers security teams with the insights they need to proactively protect their critical assets, prevent fraud and data breaches, protect their brand, conduct investigations in real-time and minimize attack surface. With easy integrations to the organization's security stack, Sixgill delivers clear visibility into the organizational threatscape coupled with contextual and actionable recommendations for remediation - all from a single pane of glass.

Analysts can stay ahead of the curve and alleviate "alert fatigue", pinpoint the golden nugget of threat intelligence and drive knowledge across the organization.

Security teams can easily search and deep-dive into unmatched intelligence data, prioritize and respond to threats targeting critical business assets and systems in the organization - in real-time. They get actionable insights to mitigate and remediate threats. They can conduct in-depth threat intelligence investigations, reduce risk exposure/incidents and minimize damage.

Chief Risk Officers can gain insight into the business impact of cyber vulnerabilities, threats, exposures and risks. They can better assess digital risks and manage risks wisely, getting actionable intelligence to prioritize and deal with threats and events.

7x
DETECTION
of leaked credentials

Up to **10x**
COLLECTION
from dark web sources

13x
COLLECTION
from instant messaging apps

24x
FASTER EXTRACTION

Features and functionalities

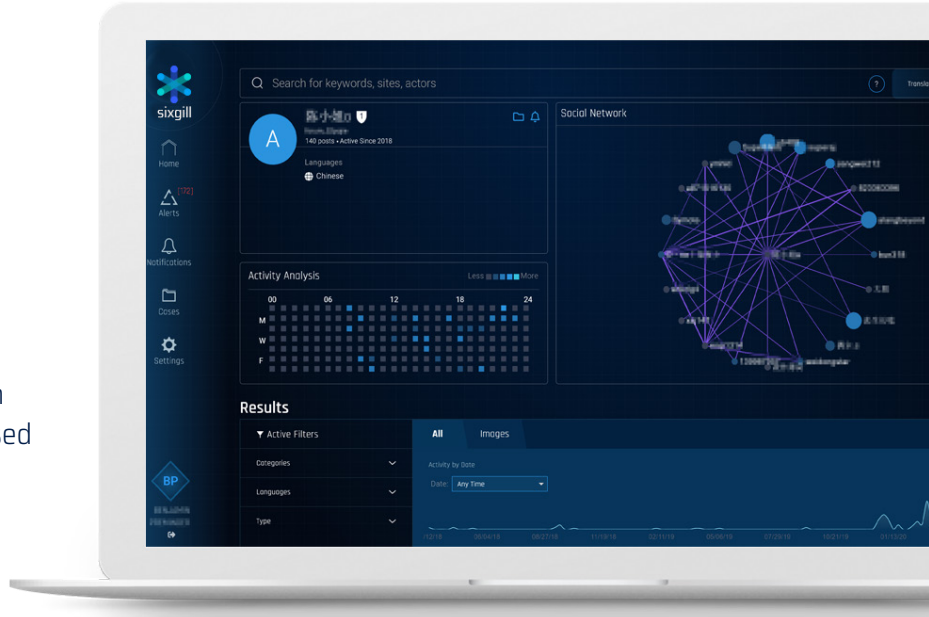
Sixgill is the only solution that provides threat intelligence teams with fully automated threat intelligence life cycle and ad-hoc investigation in real-time.

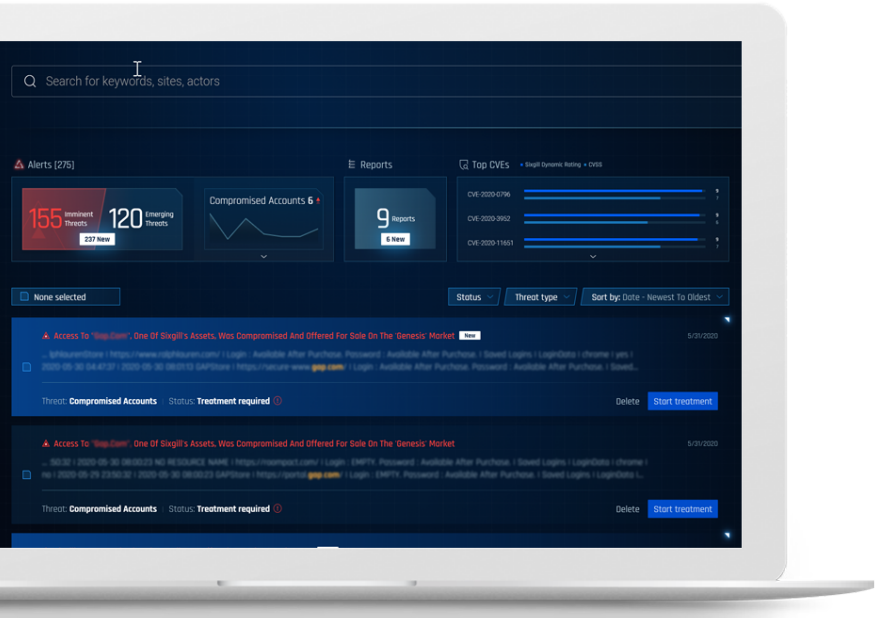
REAL-TIME AND AD-HOC ACCESS

- Thousands of correlated sources from the deep, dark and surface web, powered by a proprietary Natural Language Processing (NLP) algorithm.

MACHINE LEARNING DATA ENRICHMENT PROCESS

- A unique algorithm that correlates datasets with client assets, and prioritizes security actions based on real threats.
- Advanced image processing for intelligence extraction from images.





SAAS VISUALIZED INVESTIGATIVE PORTAL

- Quickly fill in the blanks and build the entire threat picture like never before.
- Deep dive into any escalation in real-time and understand the context. Research threat actor's profile, MO and history. Review and analyze across languages, sites, timeframes, types of products, topics, entities, and more.

CONTEXTUAL AND ACTIONABLE

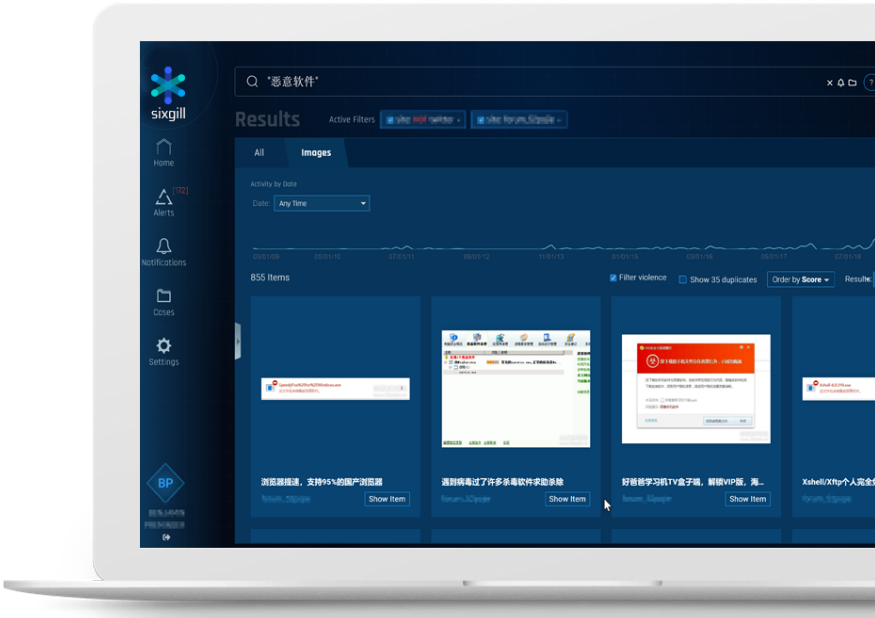
- Elevating tactical intelligence to become operational and strategic. By providing context, Sixgill helps security teams understand how each item is related to tactics, techniques and procedures of specific threat actors.

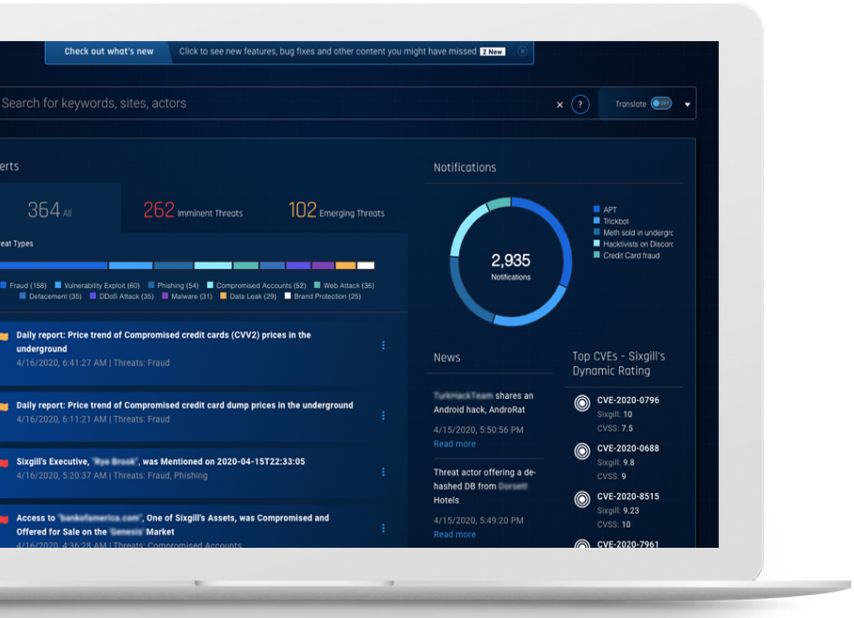
OUT-OF-BOX READINESS, INSTANT TIME TO VALUE

- Pre-configured and automatically updated alerts and insights according to vertical and use case. Automatic mapping of your assets for triggering imminent threat alerts.
- Fully and automatically integrated into the enterprise ecosystem and security stack.

CENTRALIZED, MULTI-TENANT AND ROLE-BASED ARCHITECTURE FOR DIRECT AND MSSPS:

- MSSPs can harness Sixgill's threat intelligence solutions to provide customers with a customized array of threat intelligence services with total data separation between customers in a single deployment.
- IT security, threat intel analysts and operations users can use the UI for deep investigation across a wide array of datasets.





NEW UI: TOTAL VISIBILITY IN A SINGLE PANE OF GLASS:

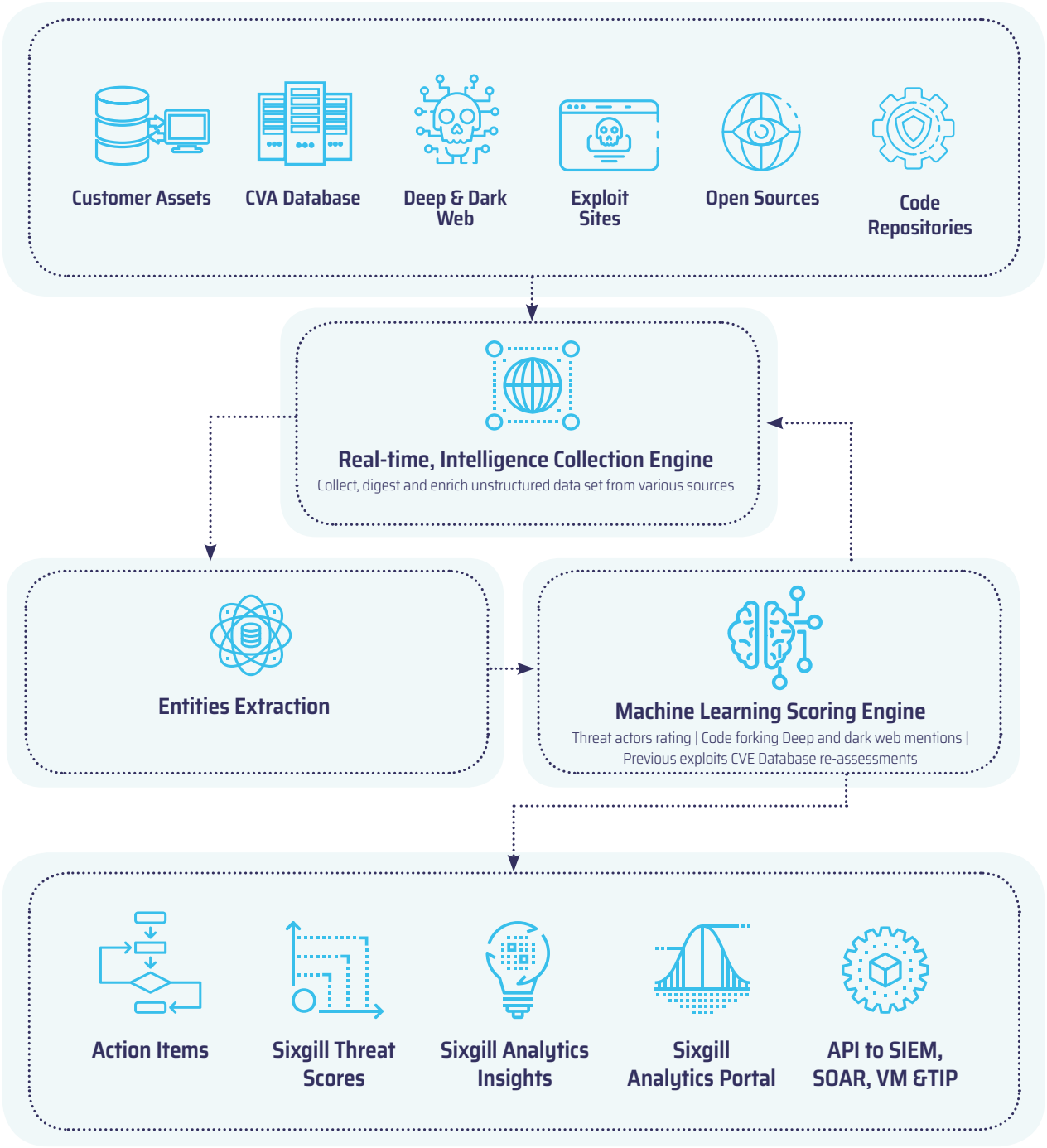
- The single pane of glass dashboard design allows ongoing visibility into your digital systems, assets and data, at a glance, for thorough protection. Easy to use and operate, the UI includes Google-like search functionality to quickly drill down, investigate events and understand activities.
- Security Teams can use it to gain total visibility into their cyber security posture from a single pane of glass.
- CROs can determine and refine their risk assessments based on cyber resilience scores and actionable insights to improve posture and reduce risk exposure.
- IT security, threat intel analysts and operations users can use the UI for deep investigation across a wide array of datasets.

> **"Sixgill's intel collection is unique, relevant, and accurate. Also, the portal provides context: source, actor, and post title - which is key. By getting the full picture, I can easily investigate emerging threats and efficiently produce meaningful insights that matter to my organization."**

Threat analyst, financial services leader

Architecture and Integrations

Sixgill easily and seamlessly integrates with all major TIP, SIEM, SOAR, Firewall and VM platforms. It is a cloud based, SaaS solution that layers on top of your enterprise core security stack to provide a total integrated solution.



Common use-cases

Sixgill can be deployed in various scenarios. It features a centralized, multi-tenant and role-based architecture for direct use as well as MSSPs. Organizations from all sectors can use Sixgill to tackle a wide range of scenarios.

Compromised credentials	Alerts of leaked credentials of its employees. These credentials were either posted on the underground, or were part of a leaked DB that was shared or sold on the underground
Cyber incidents detection + incident response	Investigate a specific threat or incident across wide datasets from the deep, dark and surface web. Including but not limited to: enrich the investigation with context, attribute an incident to a specific threat actor, and more
Executive/VIP monitoring	Alerts if an executive is being targeted by a cyber or physical threat, including spear-phishing attacks, CEO scams, doxing, and more
Enriching endpoint protection (IOCs)	Sixgill provides security vendors with a feed of IOCs appearing on the underground (domains, IPs, Hashes etc.), enriched with context. Including but not limited to: attributing them to a specific actor, providing their risk score, and more
Vulnerability assessment	Investigate a specific vulnerability across wide datasets from the deep, dark and surface web. Including but not limited to: enrich the investigation with context, attribute a POC exploit code to a specific threat actor, and more
Fraud management (root-cause analysis)	Allow financial institutions to better implement a root-cause analysis of credit card leaks and mitigation
Law enforcement terror investigations	Access dozens of terror-related forums and thousands of Telegram channels. Intuitively correlate between different datasets and create a coherent intelligence picture in real-time
Drugs and weapons investigations	Access dozens of drug and weapon related markets as well as thousands of IM channels. Intuitively correlate between different datasets in order to create a coherent intelligence picture in real-time
MSSPs	Harness the Sixgill threat intelligence structure to provide their customers with a customized array of threat intelligence services to protect their brands and organization's most critical assets

SECURITY We treat security of data with the highest standards. Sixgill's security-first approach leverages the best and most advanced technologies to make sure that your data stays safe and private. Our service undergoes rigorous audits and employs the latest best practices to ensure the integrity of the data as well as its authenticity, security and compliance.

sixgill

Sixgill is a fully automated threat intelligence solution that helps organizations protect their critical assets, reduce fraud and data breaches, protect their brand and minimize attack surface. The portal empowers security teams with contextual and actionable alerts as well as the ability to conduct real-time investigations. Rich intelligence streams such as Darkfeed harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include enterprises, financial services, MSSPs, government and law enforcement entities.

www.cybersixgill.com