cybersixgill

JOINT SOLUTION

CrowdStrike & Darkfeed Integration: A quantum leap in threat intelligence

Modernized threat intelligence for next-level protection

Darkfeed + CROWDSTRIKE

Key Solution Benefits:

- **Automatically Enrich IOCs** from CrowdStrike Falcon (machine-to-machine)
- **Gain unparalleled context** with essential explanations of IOCs
- **Supercharge CrowdStrike Falcon** with seamless integration of real-time contextual data from the most comprehensive coverage of deep and dark web sources
- **Proactively analyze and investigate** new malware threats as they emerge
- **Get actionable insights to** effectively mitigate threats and better understand malware
- **Level up your threat hunting** for malicious IOCs in corporate networks

Challenges

Today's manual approach to cyber intelligence is flawed. It focuses on manual and generic collection, and indexing and labeling that is not tailored to the agency's Priority Intelligence Requirements (PIRs). Security and investigative teams, acting on data and methodologies that are getting more and more obsolete by the minute, are failing to provide comprehensive and efficient security to their organizations.

Solution

Darkfeed is the industry's most comprehensive, automated IOC enrichment solution available on the market today. With Darkfeed, CrowdStrike users can get early warnings of threats and block items that compromise their organization. Powered by Cybersixgill's unparalleled data lake from the deep and dark web, it delivers contextual and actionable insights to proactively block threats and enrich endpoint protection in real-time – straight from the CrowdStrike dashboard.

By coupling Darkfeed's IOC information with Cybersixgill's Investigative Portal, users can further probe threat actors and contexts most relevant to their organizations most critical assets.

Use case	Solution Description	Benefits
Incident response	Automatically integrate IOCs into their security solutions (machine-to-machine)	Receive early warnings of new threats as they develop on the dark web before they are weaponized
Zero Day malware research	Hunt for malicious indicators of compromise in organizational networks	Conduct deep analysis of malware available for download on the deep and dark web

Continuous and real-time: visibility and context

The Cybersixgill and CrowdStrike integration makes it easy to gain deeper visibility and advanced context for IOCs from the deep and dark web — providing an enhanced level of detection and protection for your organization and its critical assets.

Fuel Your Analytics

Use the data to track, trend and gain data-driven actionable insights to the IOCs collected by Darkfeed. Gain better understanding of malware TTPs and trends.

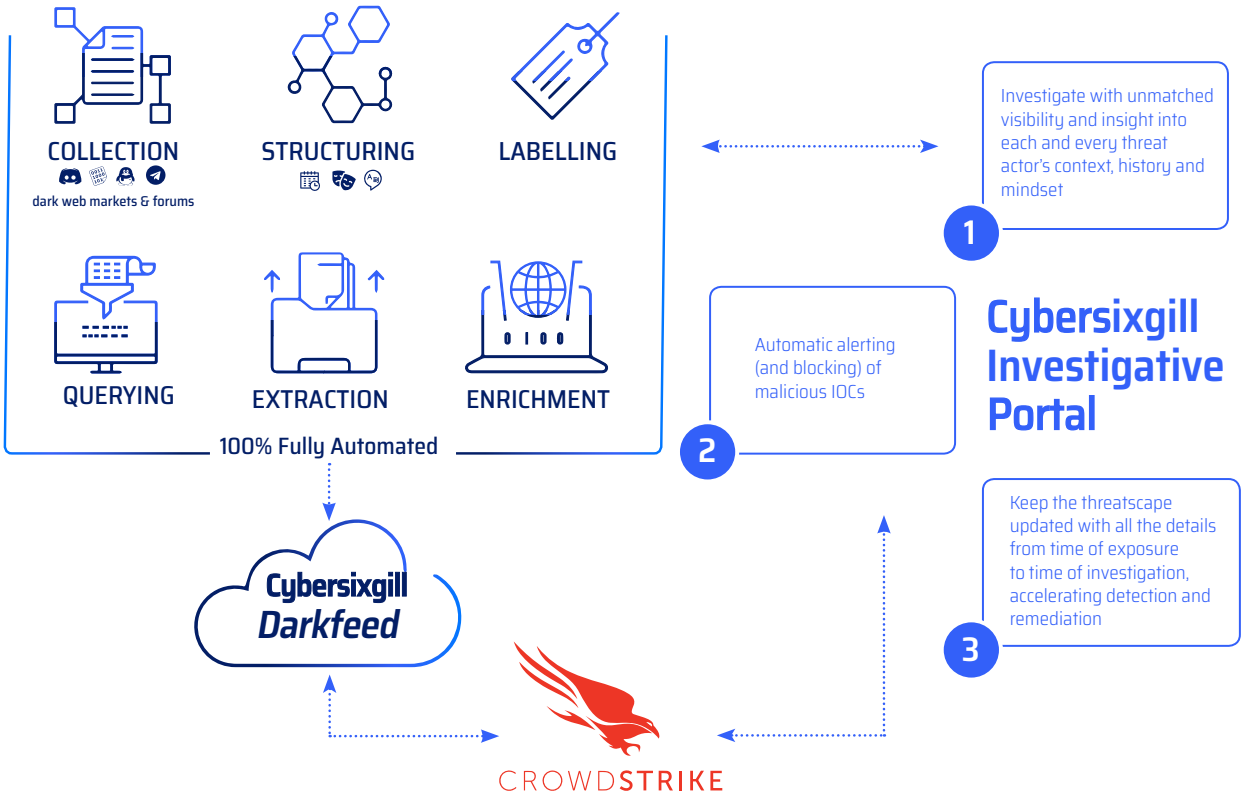
Visibility Into Your Threatscape

Gain total visibility of the threatscape of your industry. Mitiigate threats in advance, prevent incidents and minimize attack surface.

> **“Integration with Cybersixgill allows you to automate incident enrichment, which saves significant time for security analysts and speeds up investigation and incident resolution.”**
>
> *Senior Threat Analyst*

SECURITY We treat security of data with the highest standards. **Cybersi**xgill’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.

How CrowdStrike Falcon and Cybersixgill Work Together



CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

cybersixgill

Cybersixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response – in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations. Rich data feeds such as Darkfeed™ and DVE Score™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems. Most recently, Cybersixgill introduced agility to threat intel with their CI/CP methodology (Continuous Investigation/Continuous Protection). Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

To learn more, visit www.cybersixgill.com and follow us on Twitter: @cybersixgill and LinkedIn.