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.

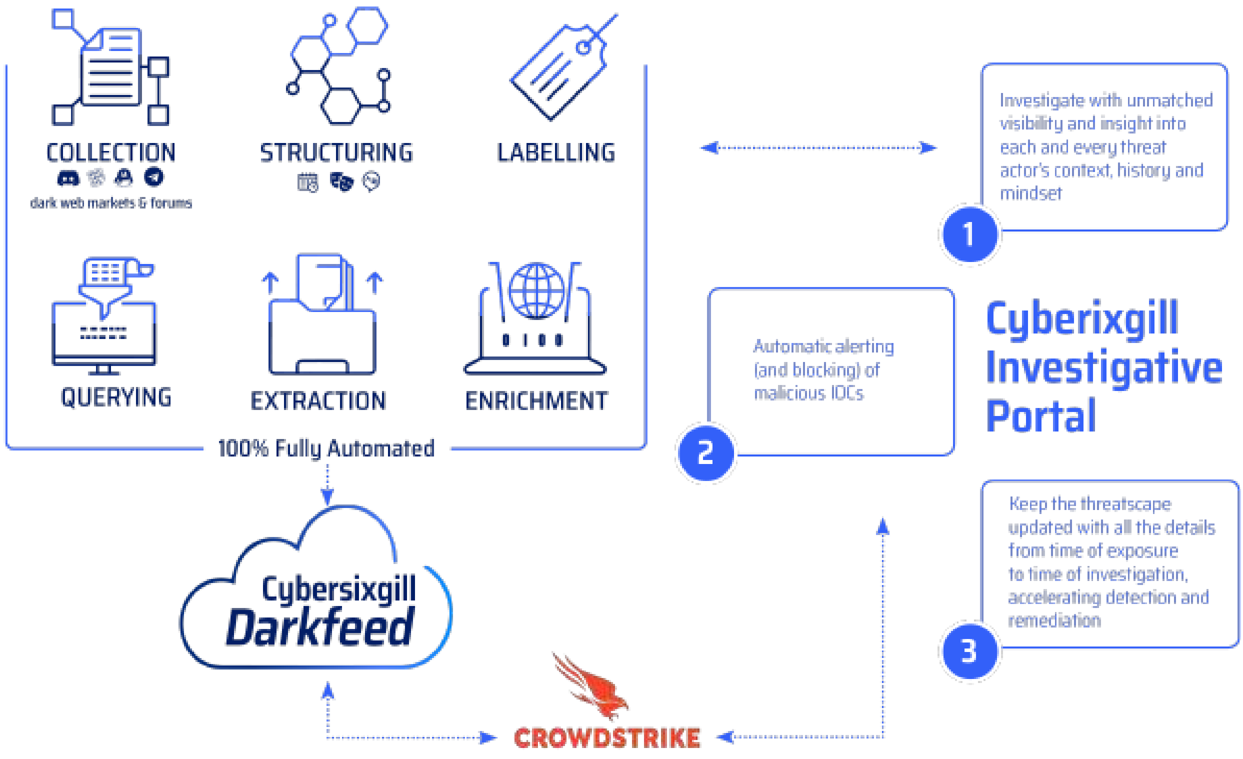
Visibility Into Your Threatscape

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. Cybersixgill’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



COLLECTION

dark web markets & forums

STRUCTURING

LABELLING

QUERYING

EXTRACTION

ENRICHMENT

100% Fully Automated

Cybersixgill Darkfeed

CROWDSTRIKE

1 Investigate with unmatched visibility and insight into each and every threat actor's context, history and mindset

2 Automatic alerting (and blocking) of malicious IOCs

3 Keep the threatscape updated with all the details from time of exposure to time of investigation, accelerating detection and remediation

Cyberixgill Investigative Portal

CROWDSTRIKE

CrowdStrike is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud, the Falcon platform enables partners to rapidly build best-in-class integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

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

cybersixgill

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, Darkfeed™ enriches endpoint protection by preemptively blocking malicious IOCs, while CVE insights from the DVE Score™ 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.

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