JOINT SOLUTION

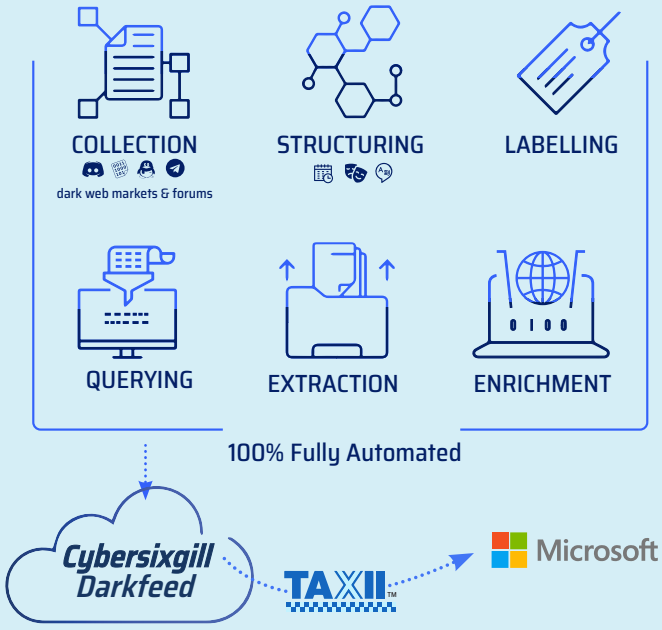
Azure Sentinel and Darkfeed: the future of threat intelligence

Darkfeed + Microsoft

www.cybersixgill.com

Benefits

- **Automatically enrich IOC** from Azure Sentinel or integrate Darkfeed into Azure Sentinel (machine-to-machine)
- **Gain unparalleled context** with essential explanations of IOCs
- **Power-up Azure Sentinel** with seamless integration of real-time contextual data
- **Get actionable insights** to effectively mitigate threats
- **Level up your threat hunting** for malicious IOCs in corporate networks
- **Better understand** malware TTPs and trends



ABOUT CYBERSIXGILL'S DARKFEED

Darkfeed is the industry's most comprehensive deep and dark web threat intelligence stream. With Darkfeed, Azure Sentinel users can get real-time warnings about malicious IOCs, and block items that threaten their organization.

It harnesses Cybersixgill's unmatched intelligence collection capabilities both in terms of breadth and quality. Darkfeed's contextual threat intelligence is highly accurate, comprehensive, covert and automated.

The feed is structured in the STIX format, using TAXII protocol to allow Azure Sentinel users to automatically consume and integrate it with their security systems, processes and methodologies.

> **"Darkfeed is our fraud teams' magic bullet of real-time intelligence. It has transformed our ability to understand and minimize digital risk across the entire organization".**
>
> *CISO, Fortune 1000*

cybersixgill

Unleash Azure Sentinel with real-time intelligence:

Automatically integrate IOCs into Azure Sentinel
to stay ahead of attacks

Receive early warnings
of new threats as they develop on the dark web, before they are deployed in the wild

Hunt for malicious IOCs
in organizational networks right from the Azure Sentinel dashboard

Conduct deep analysis of malware
available for download on the deep and dark web

Preempt potential threats across your environments

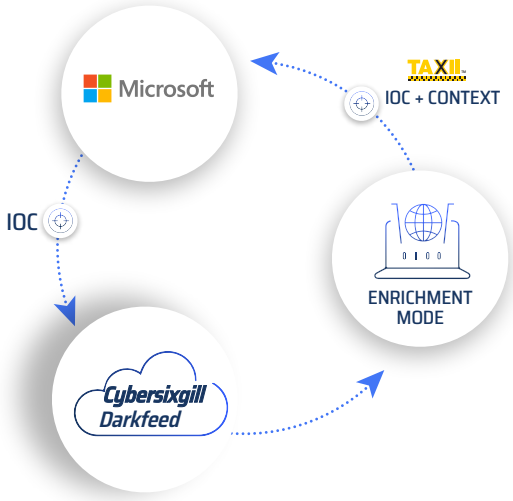
Use the data to track, trend and gain data-driven actionable insights to the IOCs collected by Darkfeed to prevent, detect and respond to potential threats across your environments.

360° Threat Visibility

Gain total visibility of the threatscape of your industry. Mitigate threats in advance, prevent incidents and minimize attack surface. Gain better understanding of malware TTPs and trends.

Azure Sentinel Enrichment mode: unparalleled context from Darkfeed

- Automatically enrich IOCs from Azure Sentinel (machine-to-machine) through Darkfeed
- Gain unparalleled context with essential explanations of Azure Sentinel's IOCs
- Secure communication in Trusted Automated Exchange of Intelligence Information (TAXII™) protocol



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.

ISO TAXII STIX

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**

Microsoft

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Azure Sentinel is your birds-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI). Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs—while reducing IT costs.