

JOINT SOLUTION

# Splunk Enterprise Security and Darkfeed - next-level threat intelligence

Darkfeed + splunk>

www.cybersixgill.com

## Benefits

- **Automatically integrate IOC** into Splunk (machine-to-machine)
- **Supercharge Splunk Enterprise Security** with seamless integration of real-time contextual data
- **Receive automated early warnings** of new malware threats
- **Get actionable insights** to effectively mitigate threats
- **Level-up your threat hunting** for malicious IOCs in corporate networks
- **Better understand** malware TTPs and trends



100% Fully Automated



## ABOUT CYBERSIXGILL'S DARKFEED

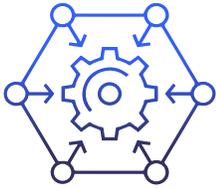
Darkfeed by Cybersixgill is the industry's most comprehensive deep and dark web intelligence stream of IOCs. With Darkfeed, Splunk users can get early warnings of malware threats and block items that threaten their organization. It harnesses Cybersixgill's unmatched intelligence collection capabilities 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 allowing Splunk users to automatically consume and integrate it with their security systems, processes and methodologies.

“Darkfeed is a game-changer for Splunk users. Supercharging Splunk with real-time threat intelligence drives the ability to understand and minimize cyber risk across the entire organization like never before.”

CISO

# Unleash Splunk with Real-Time Intelligence



## Automatically integrate IOCs

to supercharge your threat intelligence



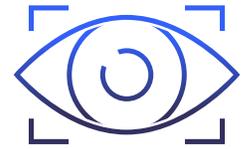
## Receive early warnings of new threats

as they develop on the dark web, before they are deployed in the wild



## Hunt for malicious IOCs

in organizational networks right from the Splunk dashboard



## Conduct deep analysis of malware

available for download on the deep and dark web

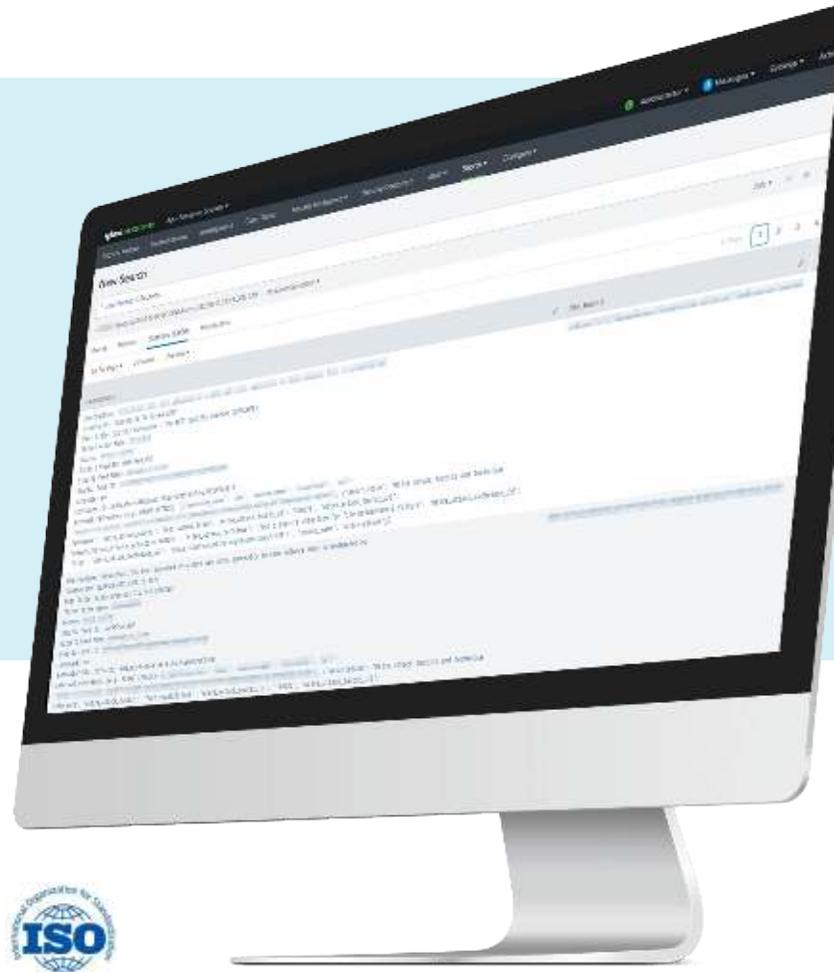
## FUEL YOUR ANALYTICS

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. Mitigate threats in advance, prevent incidents and minimize attack surface.

**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.



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.



Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable. Join hundreds of thousands of passionate users by trying Splunk solutions for free:

<http://www.splunk.com/free-trials>.