ANOMALI AND SIXGILL DARKFEED: NEXT-GEN THREAT INTELLIGENCE

Detect and respond to threats operating in the deep and dark web with Sixgill and Anomali

SIXGILL AND ANOMALI JOINT SOLUTION FEATURES:

- Anomali harnesses Sixgill's threat intelligence to improve cyber-security decisions, reduce risk and strengthen defenses.

- Darkfeed supercharges Anomali with unmatched threat intelligence, automatically collected from the deep and dark web.

- Together, Anomali and Darkfeed deliver the most comprehensive, real-time threat intelligence that Anomali users can leverage to make mission-critical decisions regarding cyber threats.

- With Darkfeed, Anomali users can get real-time, actionable insights and block items that threaten their organization.

IMMEDIATE TIME-TO-VALUE

- Harness Sixgill'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 intelligence stream is structured in the STIX format allowing Anomali users to automatically consume and integrate it with their security systems, processes, and methodologies.

- Reduce risk of data breaches, IP theft, ransomware, and other cyberattacks.

UNLEASH ANOMALI WITH REAL-TIME INTELLIGENCE

Fuel your analytics: Use the intel to track, trend, and gain data-driven actionable insights into the IOCs collected by Darkfeed. Gain better understanding of malware tactics, techniques, and procedures.

Get visibility into your threatscape: Gain total visibility of the threatscape of your industry. Mitigate threats in advance, prevent incidents, and minimize attack surface.

Security-centric approach: We treat the 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.

AUTOMATICALLY INTEGRATE IOCS INTO ANOMALI

To supercharge your threat intelligence

RECEIVE EARLY WARNINGS

Anticipate new threats as they develop on the dark web before they are deployed in the wild

CONDUCT DEEP ANALYSIS OF MALWARE

Available for download on the deep and dark web

CASE STUDY: IMMINENT THREATS TO YOUR ASSETS

CHALLENGE:

A client's SOC was facing severe challenges by relying on manual intelligence feeds. It was either irrelevant (dated), or inaccurate (loaded with false-positives). This created gaps and bottlenecks, with analysts collapsing under the volume of manual work required to produce quality intelligence.

- Dated, irrelevant and inaccurate threat intelligence, hindering their ability to perform optimally
- Constant information fatigue due to data overload
- Lack of context and visibility into an attacker mindset

SOLUTION:

As part of an effort to accelerate time-to-intel and optimize workflows, the company chose Darkfeed™. With Darkfeed, the CSIRT teams were able to:

- Preemptively identify and block threats
- Substantially reduce false-positives
- Maximize security systems' effectiveness
- Understand the full picture behind malicious threat vectors
- Dramatically reduce response time and number of attacks

CUSTOMER BENEFIT:

Initially embraced by CSIRT teams, they integrated Darkfeed into their Anomali platform and began to see clear and instant value. Later usage was expanded to additional threat intelligence teams who began using Sixgill's portal, and the value grew exponentially.

BENEFITS

- Get actionable insights to effectively mitigate threats
- Level up your threat hunting for malicious IOCs in corporate networks
- Hunt for malicious IOCs in organizational networks right from the Anomali dashboard
- Automatically integrate IOCs into Anomali (machine-to-machine)
- Supercharge Anomali with seamless integration of real-time contextual data
- Receive automated early warnings of new malware threats.

COLLECTION
Dark Web markets
Deep Web forums

STRUCTURING

LABELLING

QUERYING

EXTRACTION

ENRICHMENT

100% FULLY AUTOMATED

Darkfeed → ANOMALI

ANOMALI®