Next-gen Threat Intelligence and Incident Response

CORTEX XSOAR BY PALO ALTO NETWORKS | SIXGILL Darkfeed

In today's ever-growing cyber threatscape, security teams often find it hard to keep up. They need the best tools that can support hyper scaling of the organization as well as the threatscape: next-gen threat intelligence, combined with a sophisticated orchestration and automation platform, that also provides total visibility from a single pane of glass.

Sixgill and Cortex XSOAR are enabling customers to scale, stay ahead of the threat curve, and accelerate their incident prevention and response by combining deep and dark web intelligence with unparalleled automation. Together, they are the ultimate power tools for building a simple, automated and effective cybersecurity strategy, and executing it to the fullest extent in order to maximize outcomes and business impact.

Integration Features

- Integrate and customize an automated intelligence stream of unique, relevant indicators of compromise (IOC)
- Receive early warnings of new malware threats
- Hunt for malicious IOCs on corporate networks
- Better understand trends in the criminal underground
- Provide an extra layer of security by harnessing Sixgill's investigation platform in tandem with Cortex XSOAR, to allow deeper investigations and root-cause analys

Benefits

- Automatically integrate IOCs into Cortex XSOAR (machine-to-machine)
- Supercharge Cortex XSOAR with seamless integration of real-time contextual data
- Receive automated early warnings of new malware threats and automatically trigger the right playbooks
- Get actionable insights to effectively mitigate threats
- Level up your threat hunting for malicious IOCs in corporate networks
- Better understand malware TTPs and trends

Compatibility

Products: Cortex XSOAR, Sixgill Darkfeed

paloalto NETWORKS

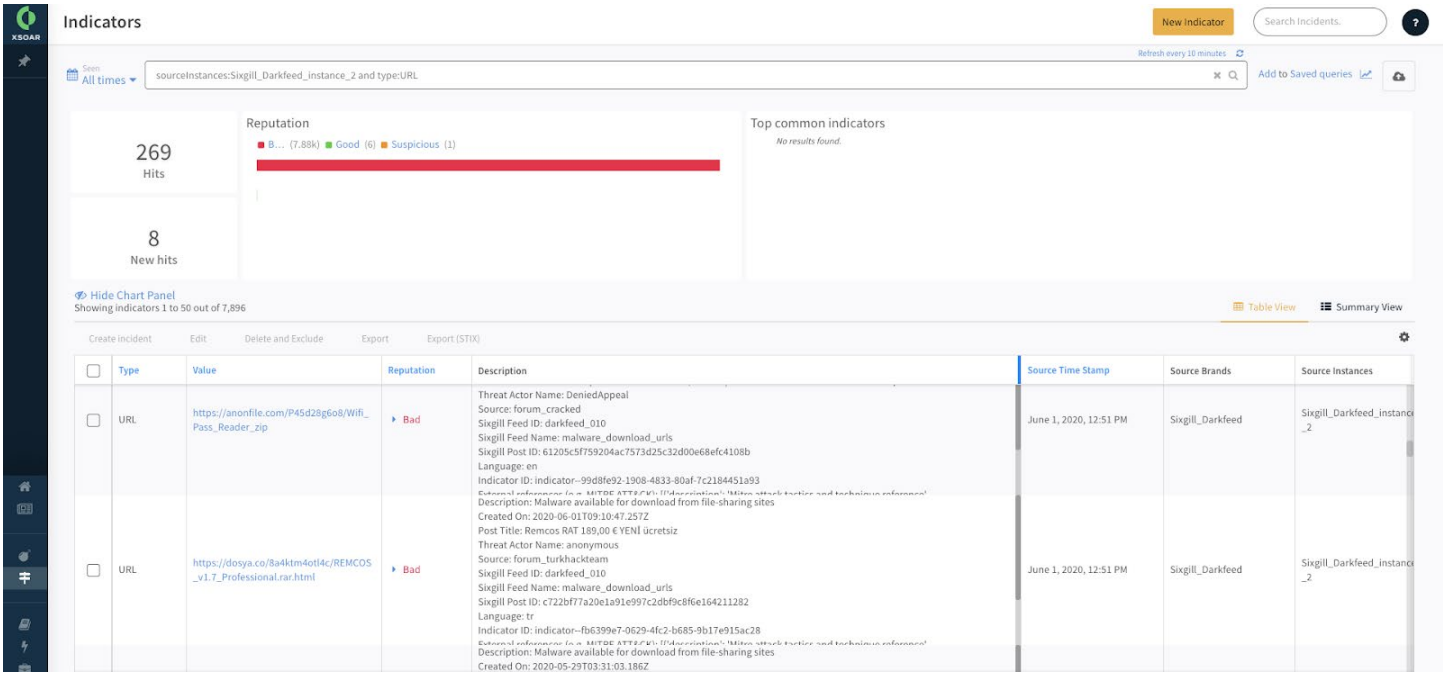
Use Case #1 Automated threat enrichment and response

Challenge: Incident response activities often include repetitive tasks based on fragmented, lacking or insufficient information. Irrelevant alerts that cause fatigue and disparate tools for different tasks all add up - SOC analysts find it very difficult to keep up.

Solution: SOCs using Sixgill Darkfeed for threat intelligence, and Cortex XSOAR for security orchestration and incident response, can automate indicator enrichment through Cortex XSOAR playbooks. These playbooks harness Darkfeed's IOCs to trigger and execute actions across the SOC's entire security stack. For example, analysts can leverage Darkfeed to enrich domains, IPs, URLs and file hashes as automatable playbook tasks.

Benefit:

1. Automation and Time-to-Intel: Cortex XSOAR playbooks coupled with Darkfeed can standardize and accelerate triage and resolution of security alerts. Analysts gain total visibility in a single pane of glass. With automatic integration of IOCs, and early warnings of new threats as they develop on the dark web, more analyst time is freed up to conduct deeper analysis of malware available for download on the deep and dark web.
2. Accuracy: Not only does the integration provide automation and speed to intel, but the nature and quality of the IOCs that Darkfeed delivers have been proven to be highly accurate. This eliminates the need to do significant follow up and a substantial verification process.
3. Uniqueness: Highly automated, ultra-fast, no need to verify, and above all, unique. Over 50-60% of the IOCs Darkfeed provides cannot be detected by other anti-virus tools.



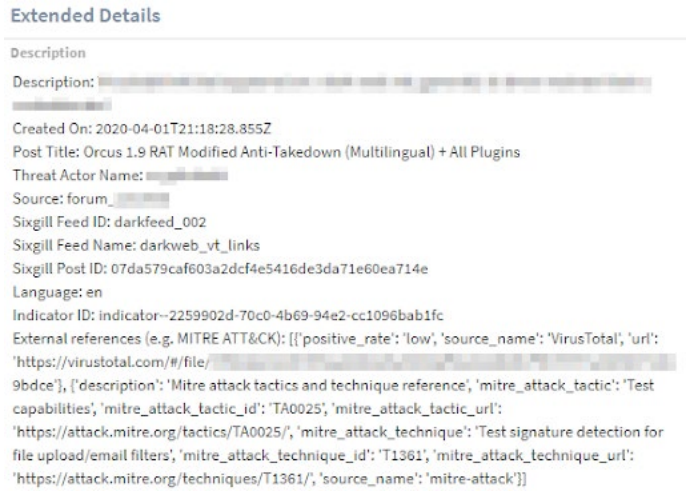
Use Case #2 Researching malware hosted on dark web file sharing sites

Challenge: The dark web is a playground of tools for aspiring attackers. Threat actors post malware and hacking tools on dark web file sharing sites and share them for anyone to download. Once in the hands of even an amateur attacker, these tools can inflict considerable damage to an organization. However, it is not simple for an analyst to manually find those malwares. They would have to be familiar with the underground's many forums and markets and need to hunt for malware samples one-by-one. This requires advanced skills and considerable time.

Solution: The Darkfeed provides its customers with URLs to malware shared on underground file sharing sites, including explanations of each item. This allows malware researchers to quickly identify, investigate, download, and analyze the arsenal of malicious tools available to threat actors on the deep and dark web, and explore them by pivoting to the Sixgill investigative portal. With this, researchers can efficiently understand emerging threats and their context in order to quickly design advanced and efficient protections against them.

Benefit:

1. Accessibility: Darkfeed closes the expertise gap in real-time. The malware researcher does not need to be an expert in deep and dark web forums in order to be able to access the malware.
2. Time-saving: This is a huge time saver for analysts that also provides them with better understanding of the organization's malware threatscape and better understanding of malware TTPs and trends.


Extended Details

Description

Description: [redacted]

Created On: 2020-04-01T21:18:28.855Z
Post Title: Orcus 1.9 RAT Modified Anti-Takedown (Multilingual) + All Plugins
Threat Actor Name: [redacted]
Source: forum_[redacted]
Sixgill Feed ID: darkfeed_002
Sixgill Feed Name: darkweb_vt_links
Sixgill Post ID: 07da579caf603a2dcf4e5416de3da71e60ea714e
Language: en
Indicator ID: indicator--2259902d-70c0-4b69-94e2-cc1096bab1fc
External references (e.g. MITRE ATT&CK): [{'positive_rate': 'low', 'source_name': 'VirusTotal', 'url': 'https://virustotal.com/#/file/[redacted]
9bdce'}, {'description': 'Mitre attack tactics and technique reference', 'mitre_attack_tactic': 'Test capabilities', 'mitre_attack_tactic_id': 'TA0025', 'mitre_attack_tactic_url': 'https://attack.mitre.org/tactics/TA0025/', 'mitre_attack_technique': 'Test signature detection for file upload/email filters', 'mitre_attack_technique_id': 'T1361', 'mitre_attack_technique_url': 'https://attack.mitre.org/techniques/T1361/', 'source_name': 'mitre-attack'}]

About Sixgill

Sixgill's fully automated threat intelligence solution helps organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response -- in real-time. Sixgill's investigative portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as Darkfeed™ harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include global 2000 enterprises, financial services, MSSPs, governments and law enforcement entities. For more information, visit www.cybersixgill.com

About Cortex XSOAR

Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/xsoar.