Siemplify & cybersixgill

SOLUTION **BRIEF**

Siemplify + Cybersixgill Darkfeed:

Level-up Threat Intelligence and Incident Response

Equip SOC teams to accelerate triage and resolution of security alerts.

Challenges

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

Cybersixgill Darkfeed enables Siemplify users 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.

Features

- ✔ Integrate and customize an automated intelligence stream of unique, relevant indicators of compromise (IOCs)
- ✔ 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 Cybersixgill's Investigation Portal in tandem with Siemplify, to allow deeper investigations and root-cause analysis

Joint Solution Benefits

- Automatically integrate IOCs into Siemplify (machine-to-machine)
- Supercharge Siemplify 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
- Better understand malware TTPs and trends

Elevate Siemplify with the most comprehensive threat intelligence in real- time.

Joint Use Cases

#1: AUTOMATED THREAT ENRICHMENT AND RESPONSE

Challenge

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

Solution

SOCs using Cybersixgill Darkfeed for threat intelligence and Siemplify for security orchestration, automation and response can automate indicator enrichment through Siemplify 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.

Benefits

Automation and Time-to-Intel: Siemplify 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.

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.

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.

#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

Darkfeed provides its customers with URLs for 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 Cybersixgill Investigative Portal. With this, researchers can efficiently understand emerging threats and their context to quickly design advanced and efficient protections against them.

Benefits

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.

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.

Siemplify

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

cybersixgill

About 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 CVE insights from 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, government and law enforcement entities.