

# Harvester Collection Automation API

## Enriching SOC automated online collections

### The Challenge: Manual Enrichment Can Hinder SOC Analyst Productivity

Data is the lifeblood of a SOC, and analysts need quick access to all types of data to respond to immediate threats and prevent future incidents. Many organizations invest heavily in SOC orchestration and automation tools, threat intelligence platforms (TIP), SIEMs and SOARs. These tools identify large numbers of potential threats and indicators of compromise, but the job of collecting additional intelligence for further analysis falls on analysts.

The ability to automate the immediate collection of relevant data when an event is identified helps significantly improve analysts' productivity and decreases SOC time to remediation. For example, when a new strain of malware is flagged, it can be automatically and safely downloaded and then forwarded to analysis tools prior to analyst engagement. Similarly, phishing domains can be monitored by automating the collection of images and screenshots, and when a look-a-like phishing site is confirmed, all of its assets can be downloaded. Or, if analysts are vetting and reviewing the collections, they can trigger a download of the phishing kit to then further investigate.

### The Solution: Enhancing SOC Automated Web-Based Collection

Authentic8's Harvester Automation API augments a SOC's automated web-based collection capabilities through:

- The ability to integrate into TIP, SIEM and SOAR content collection workflows via API
- A range of collection options including full page screenshots, files and video
- Dedicated egress network and granular fingerprint control, allowing for unattributable collection
- Storage of collections to Authentic8 Secure Storage, with File API for file download automation
- API task management and audit logging for administrators

### The Benefits

- Automate and easily scale repetitive or time-sensitive content gathering activities by analysts
- Enhance obfuscation and security of all automated collections
- Remove overhead of hosting, managing and maintaining homegrown "dirty" networks