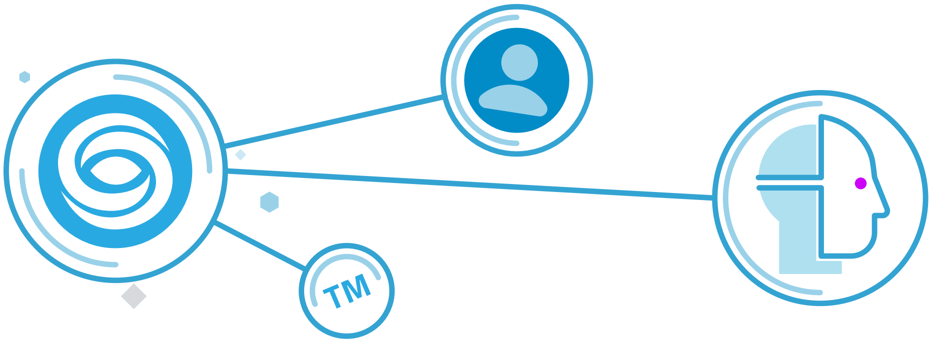
INTSIGHTS
Defend Forward™

Takedown Services

Instantly Eliminate Malicious Content

Take down external threats before they cause damage

As organizations adopt new digital channels to reach customers, cybercriminals follow suit by impersonating popular brands, promoting scam campaigns, and profiting from unknowing consumers. Organizations must extend their external monitoring and enforcement to take down campaigns that impersonate brand, infringe on trademarks, and threaten customers. IntSights provides an **in-house automated remediation service** that enables customers to take down malicious content published on the web.



Accelerate Threat Removal

Utilize our dedicated team of takedown experts to gather prerequisites, accelerate requests, and streamline workflows with your legal team so malicious campaigns are taken down as quickly as possible.

Scrub File Sharing and Paste Sites

Continuously monitor code and file sharing sites like Pastebin, Ghostbin, and GitHub, to identify exploits, sensitive data, or leaked credentials and initiate removal requests.

Leverage the broadest ecosystem of sources

IntSights addresses threats from the widest variety of sources, including social media, app stores, domain registrars, paste sites, web hosting providers, and more. We continue to develop new partnerships with registrars, app stores, and social media sites based on new attack vectors and hacker trends.

Takedowns we execute

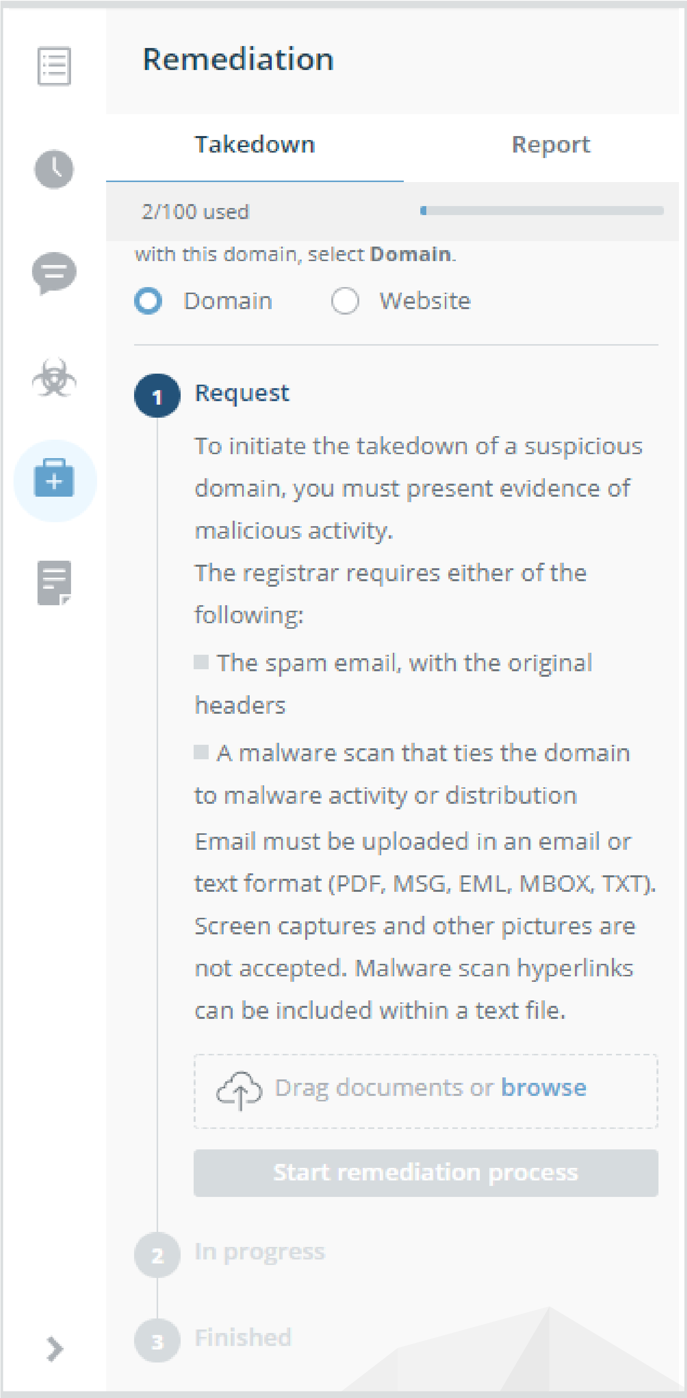
- Fraudulent social media pages impersonating a customer
- Fake and/or suspicious mobile applications posing as a legitimate customer application
- Pastes that contain sensitive data and/or any attack intention
- Domains that were involved in phishing campaigns against IntSights customers or their customers
- Phishing websites posing as a customer
- Files or malicious items involved in phishing or malware attacks against a customer
- Google search results leading to phishing websites and fraudulent activities
- Personal information of our customers' executives

INTSIGHTS
Defend Forward™

How It's Done

IntSights provides this service by contacting the website owner or domain registrar in order to have the malicious item removed or suspended. IntSights works directly with the website owner or registrar and provides the characteristics of the suspicious content. We ask customers to provide us with appropriate information, depending on the nature of the takedown request. For social media sites, for instance, the fake profile must clearly resemble the customer's graphical content, logos, industry, etc. For domains, evidence of malicious intent must be provided before it can be removed.

In addition to the automated process, the IntSights Remediation Team monitors the process and intervenes as needed when there is not a direct confirmation of the takedown or when additional information is required.



with this domain, select **Domain**.

● Domain ○ Website

1 Request

To initiate the takedown of a suspicious domain, you must present evidence of malicious activity.
The registrar requires either of the following:

- The spam email, with the original headers
- A malware scan that ties the domain to malware activity or distribution

Email must be uploaded in an email or text format (PDF, MSG, EML, MBOX, TXT). Screen captures and other pictures are not accepted. Malware scan hyperlinks can be included within a text file.

Get Started

The IntSights cloud-based **External Threat Protection Suite** requires no software to install and works across all web browsers.

Learn more about how IntSights Threat Command can help you build a better cyber defense.
Request a demo today.

Have questions? Contact us at info@intsights.com or visit us at www.intsights.com.