Remediation Services Overview

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. To stay ahead of these threats, your organization must proactively extend external monitoring and enforcement to take down campaigns that impersonate your brand, infringe on trademarks, and threaten customers. Threat Command's in-house Automated Remediation Services can help you expedite take down of malicious web content targeting your business.

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.

Continuously Identify Leaked Code

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

Leverage the Broadest Protection Coverage

Threat Command offers the widest variety of coverage, 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, so your organization is protected from emerging threats.

Takedown Services Explained

Threat Command remediation includes the following coverage areas:

- 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 our customers or their customers
- Phishing websites posing as a customer
- Files or any malicious items involved in phishing or malware attacks against a customer
- Google search results leading to phishing websites and fraudulent activities
- Unauthorized use of company trademarks (Advanced Remediation Service, see page 5)

This is a customer initiated service provided by Rapid7, in which we contact the website owner or domain registrar on behalf of the customer to have the malicious item removed or suspended. The success rate is in large part due to Rapid7's cooperation with the website owner or registrar and our ability to provide characteristics of the suspicious content. For social media sites, 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.

Workflow

Remediation requests can be submitted for all of the source types mentioned in the next section (given they are listed as "clear web").

If a customer receives an alert that is eligible for a takedown, the user can press the Remediate button to request that Threat Command have it removed from the web.

Once a request is submitted, an auto-request is sent to the source of the alert (for phishing domains and websites, the request will be sent to the registrar) along with all necessary attachments (e.g., evidence for phishing domains, trademarks for social media, etc.)

After the request is submitted, Threat Command automatically monitors the status of the request on an hourly basis to confirm that the page has been successfully removed. Once the alert has been remediated, the customer receives a notification, and the task is closed accordingly.

In addition to the automatic process, the Threat Command Remediation Team monitors the process and intervenes as needed when there is not a direct confirmation of the takedown or when any additional info is needed.

What Source Types Are Covered by Threat Command?

Rapid7 has developed partnerships with various social media sites, domain registrars, and application stores to expedite the takedown process when malicious content is discovered. Alerts originating from the following source types are available for a potential takedown:

PLATFORMS	SUPPORTED SPECIFIC SCENARIO
Mobile App Stores	Malicious application stores resembling company assets
Google Play	Malicious application resembling company assets
Facebook	Attempted job scam post using company-associated identity
	Company executive suspicious social media VIP profile
	Suspicious Social Media Profile Indication of scam intent
	Suspicious Social Media Profile, Unauthorized Brand Use
	Suspicious Social Media Profile, Unauthorized use of company trademark on a social media profile
Flickr	Suspicious Social Media page, Unauthorized Brand Use
GitHub	Company software code leaked
Instagram	Company executive suspicious social media VIP profile
	Suspicious Social Media Profile, Unauthorized Brand Use
	Suspicious Social Media Profile, Unauthorized use of company trademark on a social media profile

PLATFORMS	SUPPORTED SPECIFIC SCENARIO
LinkedIn	Suspicious Social Media Profile, Attempted job scam using company-associated identity
	Company executive suspicious social media VIP profile
	LinkedIn profile impersonating VIP company employee
	Suspicious Social Media Profile, Unauthorized Brand Use
	Suspicious Social Media Profile, Unauthorized use of company trademark on a social media profile
Pastebin	A company asset listed on a target list
	Company employee credentials leaked from a 3rd party service
	Company employee private details leaked
	Company executive login credentials leaked
	Company executive Phishing Email detected
	Company sensitive data leaked
	Potential Phishing Email
Phishing Domain	Suspected Phishing Domain
Phishing Email Account	Potential Phishing Email
Phishing Website	Company Phishing Website
Pinterest	Suspicious Social Media Page, Unauthorized Brand Use
Tiktok	Suspicious Social Media Page, Unauthorized Brand Use
Tumblr	Suspicious Social Media Profile page, Unauthorized Brand Use
Twitter	Company executive suspicious social media VIP profile
	Suspicious Social Media Profile, Unauthorized Brand Use
	Suspicious Social Media Profile, Unauthorized use of company trademark on a social media profile
Veoh	Suspicious Social Media video, Unauthorized Brand Use
Vimeo	Suspicious Social Media page, Unauthorized Brand Use
Virus Total	Company confidential documents leaked
VK	Suspicious Social Media Profile/Page/Paste, Unauthorized Brand Use
Webio	Suspicious Social Media Page, Unauthorized Brand Use
YouTube	Suspicious Social Media Channel / Video, Unauthorized Brand Use

Advanced Remediation Service

In cases where a customer wants Threat Command to remediate a threat currently unsupported by the standard remediation plan, the Advanced Remediation Services plan can be leveraged to request that the Threat Command Remediation Team attempt to take down the specific threat.