RAPID7

Remediation Services Overview

Contents

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. In fact, 91 percent of breaches start with phishing. 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 takedowns of malicious web content targeting your brand.

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 to ensure that your organization is always protected from emerging threats.

Takedown Services Explained

Threat Command's average Remediation Success Rate is 91% and includes the following coverage areas:

- Domains that were involved in phishing campaigns against our customers or their customers
- Phishing websites posing as a customer
- Fraudulent social media pages impersonating a customer, including fake job offers
- Fake and/or suspicious mobile applications posing as a legitimate customer application
- Pastes that contain sensitive data and/or any attack intention
- Suspicious email account 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

The service is provided by contacting the website owner or domain registrar in order to have the malicious item removed or suspended. The success rate is based on Threat Command' 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 relevant vendor) 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.

Source Types Covered by Threat Command

Threat Command has developed partnerships with various social media sites, hosting providers, domain registrars, and application stores to expedite the takedown process when malicious content is discovered. Alerts originating from these source types are available for takedown:

- WHOIS records (phishing domains and phishing websites)
- Social media networks (Facebook, Instagram, LinkedIn, Pinterest, TikTok, Tumbler, Veoh, Vimeo, VK, Weibo, Twitter, Telegram, Flickr, YouTube, RocketReach)
- Mobile application stores
- Online boxes and file sharing links used for malware distribution
- Online forms
- Suspicious email accounts
- Paste sites

Malicious Domains

Source Type Description

Threat Command automatically detects suspiciously registered domains that are similar to our customers' assets. Domains that can be remediated have the following criteria:

- **Domains involved in direct phishing activities or malware distribution:** These domains are actively used for distinct malicious activities. These activities can include spam emails impersonating legitimate entities requiring payments or spreading malware.
- **Domains registered by known malicious registrants:** Some registrants are known to register domains intentionally for cybersquatting purposes. These registrants (for example, Michael Ard and VistaPrint) are known within the internet industry, and some are involved in lawsuits stemming from their activities.
- **Malware-related domains that don't use customers' assets:** This type of alert will not be picked up automatically by our system but will be reported by a customer once the domain is used in an attack. Same as above, we will need a sandbox/malware analysis report as evidence in order to have the domain suspended.

Notable Registrars

GoDaddy, Cloudflare, Namecheap, Tucows

Success Rate

Once sufficient evidence is provided, the success rate is 87%.

Median Resolve Time

Resolve time is five days. However, response times may vary from one registrar to another.

Prerequisites

In order to have a domain of this type removed or suspended, we will need clear evidence from the customer showing the domain's involvement in phishing activities. Evidence can include email headers of spam emails sent from the domain (preferably in .txt file per registrar's demands) and VirusTotal/URL scan malware analysis reports showing that the domain is used for malware-related activities.

Notes

Threat Command monitors domains for changes. Once a domain changes and starts resolving to a phishing website, Threat Command can initiate action to remove the website.

Fees

One credit per standard remediation request.
If you choose to cancel a request already in progress, you will still be charged one credit.

Phishing Websites

Source Type Description

Threat Command delivers alerts for websites using our customers' names and graphics for a phishing website. However, the remediation process for "Phishing Website" alerts may vary from one to another. The Remediation Team separates phishing websites into two distinct categories, each of which receives different treatment based on how the website in question is set up.

- **Security claims:** This type of request is filed when we encounter a "traditional" phishing website. It refers to a website that claims to represent the customer, using its graphics and similar domain permutation, and intends to lure users to enter their logins or other sensitive information. This typically constitutes sufficient evidence to demonstrate a phishing site, enabling us to initiate a takedown with the registrar. For cases like this, we approach the domain's registrar and request that the domain be fully suspended. Response time may vary from one registrar to another and may take a couple of days up to several weeks to resolve.
- **Copyright infringement claims and DMCA notices:** When a website does not have any login fields nor is trying to lure victims to provide personal information, we do not have sufficient evidence to demonstrate a phishing site, making our security-based claims to the registrar invalid. For these cases, we approach the hosting provider with a DMCA claim, demanding the website be removed due to copyright infringement. DMCA is a legal claim for content removal based on copyright infringement. However, responses may vary between hosting providers due to their locations. Countries have specific laws regarding intellectual property, which may affect our success rates.

Notable Hosting Providers

Cloudflare, Namecheap, Hostgator, Hostinger

Success Rate

The success rate for phishing websites of both kinds is 91%.

Prerequisites

If a case needs to be treated using a DMCA process, then a signed Letter of Authorization must be provided and trademarked, which allows us to act on behalf of the customer (a template is available for download on the platform).

Median Resolve Time

Median resolve time for phishing websites is two days. However, response times may vary from one registrar to another.

Notes

Some registrars and hosting providers may not comply with our requests due to relevant laws in hosting provider's country of origin. For example, US and European intellectual property and anti-phishing laws may not be enforced in China or Russia.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

Application Stores

Source Type Description

Application store alerts refer to mobile and desktop applications that carry our customers' brand or company names but were uploaded without their knowledge and consent. Application store alerts come from two types of major sources:

- **Official app stores:** This type includes legitimate, well-known official app stores such as iTunes, Google Play, and Microsoft App Store.
- **Pirate app stores:** Aside from the app stores mentioned above, Rapid7 covers more than 150 unofficial app stores, some of which are malicious and "pirate" by nature.

Notable Application Stores

Google Play, Apple app store, Freeapkbaixar

Success Rate

Once sufficient evidence is provided, the success rate is 87%.

Median Resolve Time

Resolve time is two days. However, response times may vary from one application store to another.

Prerequisites

Remediation is more likely to succeed if both the company Registered Trademark and a signed Letter of Authorization (LOA) are present in the Configurations page before initiating the remediation.

Notes

Due to the nature of some pirate app stores, some processes may fail due to a lack of collaboration on the part of the app store itself. These application stores do not have any reply policy and are not legally obligated to respond to us.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

Facebook and Instagram

Source Type Description

Rapid7 provides broad intelligence and remediation coverage for Facebook and Instagram. Rapid7 can remove pages and profiles impersonating our customers' legitimate pages, as well as their executives.

Posts of malicious nature can be taken down as well, as long as they include the proper law violations (such as selling credit cards, coordinating cyberattacks, etc.). Facebook and Instagram remediation are done using the following methods:

- **Trademark claims:** relevant for pages and profiles that impersonate or use trademark or brand names without approval
- **Copyright claims:** relevant for cases in which there is no available trademark for the company or for a page/profile that does not represent the company but uses any of its copyrighted works (such as logos, graphical content, etc.)
- **Impersonation claims:** relevant for pages and profiles impersonating our customers' VIPs and executives
- **Security claims:** relevant for posts of malicious nature

Success Rate

Success rate for Facebook and Instagram is 96%.

Median Resolve Time

Once a request has been immediately acknowledged, median resolve time is two days. If the case is not clear and needs further discussion, the resolve time can require up to a week.

Prerequisites

- Global trademarks must be provided by the customer in order to facilitate page takedowns.
- Pages that are associated with a certain country will require a trademark of that country to be removed. For example, a page that tends to represent the organization in Germany or has its address appearing in Germany will require a German trademark to be removed.
- Taking down impersonating profiles for VIPs and executives requires a photo ID.

Notes

For cases in which there is no graphical content in use, the success rate may depend upon the name indication and connection to the customer's business and industry. For example, a page that carries a company name that could also be a person's name might have a lower chance of being removed.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

LinkedIn

Source Type Description

The main attack vector for spear-phishing campaigns is directly impersonating company employees, typically VIPs and high-ranking executives. This can be done through various platforms and methods, with LinkedIn being the most common.

Threat Command provides intelligence and remediation coverage for the following types of content appearing on LinkedIn and SlideShare:

- Fake and suspicious LinkedIn profiles based on impersonation claims
- Fake and suspicious company pages on LinkedIn based on trademark claim

Success Rate

The success rate for these takedowns is 99%.

Median Resolve Time

The median resolve time s less than a day.

Prerequisites

Global trademarks need to be provided by the customer in order to facilitate company page takedowns.

Notes

Takedowns based on impersonation claims may vary from one profile to another due to the nature of the reported profile and its activity pattern.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

Twitter

Source Type Description

Twitter claims are trademark based, and the profiles that are considered remediable follow either of these criteria:

- A profile that carries a customer's name along with its graphical identifiers
- A profile without a photo but with the customer's exact industry-relevant trademark

Success Rate

Success rate for Twitter is 78%.

Median Resolve Time

Median resolve time is seven days.

Prerequisites

Global trademarks must be provided by the customer in order to facilitate page takedowns. Pages that are associated with a certain country will require a trademark of that country to be removed. For example, a page that represents the organization in Germany or has its address appearing in Germany will require a German trademark to be removed.

Notes

Twitter has a strict policy regarding profile removals, which may lead to fewer profile removals when the criteria mentioned in the source description section (above) are not met.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

Other Social Media Platforms

Source Type Description

In addition to the major platforms above, Threat Command provides coverage for various other social media platforms. The remediation covers both posts and impostor accounts based on impersonation and trademark claims.

A signed Letter of Authorization allowing us to act on behalf of the customer must be provided (template is available for download in the platform).

Trademark - The remediation will be more successful if both the company's Registered Trademark and a signed Letter of Authorization (LOA) are present in the Configurations.

Notable Sources

Pinterest, Telegram, Tumbler, Veoh, Vimeo, VK, Webio, Flickr, YouTube

Success Rate

Success rate is 85% but may vary between each platform.

Median Resolve Time

Median resolve time is roughly four days but may vary between each platform.

Prerequisites

Some platforms may require global trademarks from the customer in order to facilitate page takedowns.

General Note on Social Media Takedowns:

Customers with generic assets may experience lower takedown success rates. Company names that are commonly used as personal names or represent a certain industry may not be easily removed due to a lack of connection to the customer's trademark. This issue becomes more difficult when no graphics are associated with the takedown.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

Paste Sites

Paste sites offer a free platform to share anonymous content online in plain text format.

Alerts for paste sites often include target lists of employees and lists of credential leakages, including compromised employee emails and passwords. More than half of our paste alerts and remediation requests come from Pastebin.com.

Supported Source

Pastebin.com

Success Rate

The success rate for paste sites is 99%.

Median Takedown Time

The median resolve time for paste sites is less than a day

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

GitHub

Source Type Description

GitHub is a repository hosting service that provides distributed version control and source code management, using Git, a command-line tool.

Alerts for GitHub include “Company software code leaked” or “Confidential Information Exposed.”

Supported Source

GitHub.com

Success Rate

The success rate for GitHub is 86%.

Median Takedown Time

The median resolve time for GitHub is six days.

Fees

One credit per standard remediation request. If you choose to cancel a request already in progress, you will still be charged one credit.

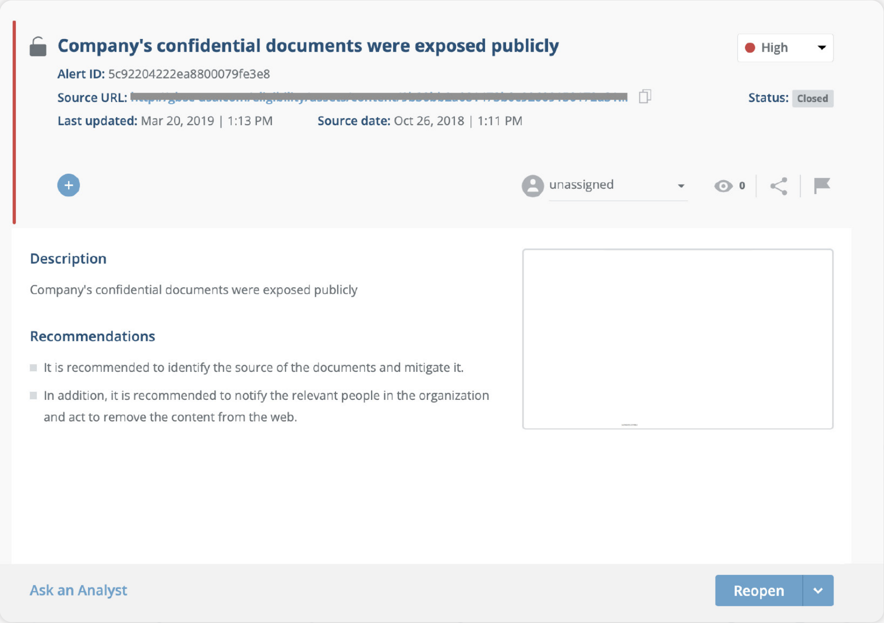
Advanced Remediation Service

Mitigating risks posed by exposed threats often requires the active removal of malicious or infringing content from various websites, platforms, app stores, and domain registrars. However, with SOC and security teams already overloaded with incoming alerts and daily tasks, managing this process end to end can be challenging. Undetected and unresolved, these risks can result in bottom-line revenue impact, financial or regulatory fines, brand and reputation damage, and erosion of customer trust.

Whoever manages this process must be persistent, possess regional expertise, and do so in a timely manner to actively minimize the attack surface and underlying risks.

> **Threat Command eliminates this burden, enabling organizations to take swift proactive actions to minimize their overall attack surface and digital risks.**

Threat Command attempts takedown requests on behalf of the requesting party for sources that cannot be supported as part of our standard remediation services. See the example below in which the “Remediate” button does not exist, indicating that the specific alert source may not be supported and cannot be taken down as part of our standard remediation services offering.



Company's confidential documents were exposed publicly

Alert ID: 5c92204222ea8800079fe3e8

Source URL: [redacted]

Last updated: Mar 20, 2019 | 1:13 PM   Source date: Oct 26, 2018 | 1:11 PM

Status: Closed

Description

Company's confidential documents were exposed publicly

Recommendations

- It is recommended to identify the source of the documents and mitigate it.
- In addition, it is recommended to notify the relevant people in the organization and act to remove the content from the web.

Example of a company confidential document exposure alert without automated remediation capability

Use Cases — Advanced Requests

1. Advanced Sources\Scenarios Coverage Request

Leveraging the standard remediation plan, the system automatically identifies and categorizes different attack types and sources, allowing customers to initiate a rapid response directly from the platform's Alert page. Threat Command addresses threats from the broadest variety of sources, including social media, app stores, domain registrars, paste sites, web hosting providers, and more. It should be noted that we continually develop new partnerships with web registrars, app stores, and social media sites based on new attack vectors and hacker trends.

However, 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 Threat Command attempt to take down the specific threat.

- **Process:**
  - In cases where Threat Command does not have experience with the source or scenario, the remediation team will investigate whether it is possible to submit a request for takedown (within two business days).
  - Assuming the takedown request can be processed by the third-party platform, the takedown request will be initiated.
- **Fee:** 5 Remediation Credits.
- **Success Rates/SLA:** May vary on a case-by-case basis.
- **Notes:**
  - Complex legal actions may require multiple formal documents for the takedown process to be initiated.
  - Successful remediation is not guaranteed and is subjected to the third-party requirements and definition for content removal.

2. Advanced Sources\Scenarios Coverage Request

In cases where customers request that Threat Command perform a threat takedown without providing sufficient evidence or necessary prerequisites, Threat Command will attempt to conduct the needed research and take down the threat. Following is the list of platforms applicable for this type of advanced remediation:

Platforms	Specific Scenario	Requirements
Facebook	VIP profile	A picture of the VIP holding ID
Instagram	VIP profile	A picture of the VIP holding ID
Suspicious App Stores	Fake App	Missing LOA
Tumblr	Page	Missing LOA
Twitter	Post	Missing LOA
	Profile (company page)	Missing LOA
	VIP profile	Missing LOA & a picture of the VIP holding ID

- **Prerequisites:** May vary on a case-by-case basis.
- **Success Rates/SLA:** May vary on a case-by-case basis
- **Fee:** 5 Remediation Credits
- **Median Resolve Time:** Typically, four days. However, response times may vary depending on source complexity.
- **Notes:** Successful remediation is not guaranteed and is subjected to the 3rd party requirements and definition for content removal.

How to Initiate an Advanced Remediation Request

To submit an Advanced Remediation Request for a takedown, see link below to our support portal, and add all the relevant information including the required files described above.

Advanced Remediation Request

Appendix 1

Mitigating risks posed by exposed threats often requires the active removal of malicious or infringing content from various websites, platforms, app stores, and domain registrars. However, with SOC and security teams already overloaded with incoming alerts and daily tasks, managing this process end to end can be challenging. Undetected and unresolved, these risks can result in bottom-line revenue impact, financial or regulatory fines, brand and reputation damage, and erosion of customer trust.

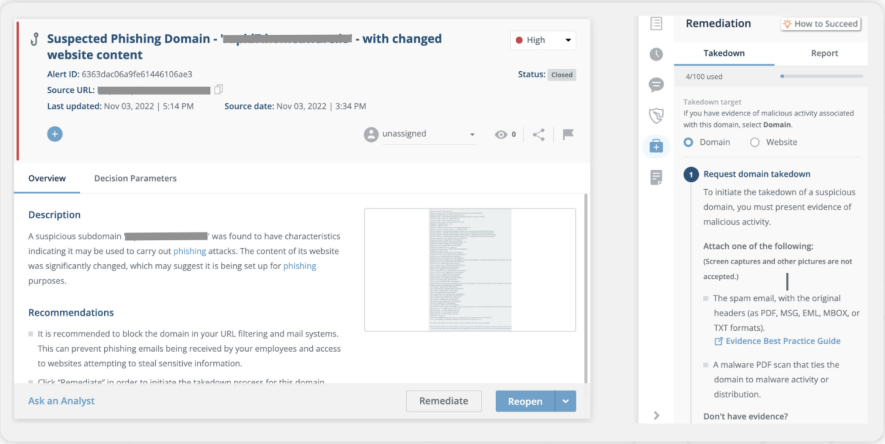
Whoever manages this process must be persistent, possess regional expertise, and do so in a timely manner to actively minimize the attack surface and underlying risks.

Remediation Requests Service:

Threat Command actively and proactively alerts customers to thousands of instances of domain impersonation, exposed sensitive data, leaked customer details, and spoofed mobile applications. Our in-house remediation and takedown service acts as a force multiplier operating as a direct extension of your SOC and security teams – offloading time-consuming analysis and investigation efforts.

Once a threat is detected and identified, customers receive an alert from Threat Command, such as domain impersonation, exposed documents, or leaked customer details. Customers can launch a remediation with a single click directly from within the Alerts page via the dedicated "Remediate" action button. This immediate action allows us to significantly limit access to a site, for example, and ultimately eliminate fraudulent content on your behalf.

If you want to insert a new source or scenario to support remediation, you must open an RFE ticket with all the relevant information. The Product team will then determine whether or not it can be taken down within the product.



Suspected Phishing Domain - '[redacted] - with changed website content

Alert ID: 6363dac06a9fe61446106ae3

Status: Closed

Source URL: [redacted]

Last updated: Nov 03, 2022 | 5:14 PM **Source date:** Nov 03, 2022 | 3:34 PM

Description

A suspicious subdomain '[redacted]' was found to have characteristics indicating it may be used to carry out phishing attacks. The content of its website was significantly changed, which may suggest it is being set up for phishing purposes.

Recommendations

- It is recommended to block the domain in your URL filtering and mail systems. This can prevent phishing emails being received by your employees and access to websites attempting to steal sensitive information.
- Click "Remediate" in order to initiate the takedown process for this domain.

Remediation

4/100 used

Takedown target
If you have evidence of malicious activity associated with this domain, select **Domain**.

● Domain ○ Website

1 **Request domain takedown**

To initiate the takedown of a suspicious domain, you must present evidence of malicious activity.

Attach one of the following:
(Screen captures and other pictures are not accepted.)

- The spam email, with the original headers (as PDF, MSG, EML, MBOX, or TXT formats).
  Evidence Best Practice Guide
- A malware PDF scan that ties the domain to malware activity or distribution.

Don't have evidence?

Figure 1 - Example of a suspected phishing domain alert with remediation capability enabled

It should be noted that Threat Command handles dozens of takedown and remediation requests daily, allowing customers to utilize our dedicated team of experts to gather prerequisites, accelerate requests, and streamline workflows so malicious content can be taken down as quickly as possible.

Product-Supported Remediation Service:

Platforms	Supported Specific Scenario
Mobile App Stores	Malicious application stores resembling company assets
Google Play	Malicious application resembling company assets
eBay	Product for sale
Etsy	Product for sale, Suspicious Social Media Profile, Unauthorized Brand Use
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
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

Platforms	Supported Specific Scenario
Phishing Domain	Suspected Phishing Domain
Phishing Email Account	Potential Phishing Email
Phishing Website	Company Phishing Website
Pinterest	Suspicious Social Media Page, Unauthorized Brand Use
Reddit	Suspicious Social Media Page, Unauthorized Brand Use
Scribd	Suspicious Social Media Page, Unauthorized Brand Use
Studylib	Suspicious Social Media Page, Unauthorized Brand Use
Telegram	Suspicious Social Media Page, Unauthorized Brand Use - Channel, Group, User, Bot. *Telegram requires proof of abuse of both the company registered trademark AND company name (one is not adequate). **Telegram policy protects the content of messages inside a group or channel, so those are not sufficient proof of abuse.
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

Unsupported Remediation Services:

Platforms	Unsupported Specific Scenario
Brand Reputation	Rapid7 does not handle takedown requests related to brand reputation since they are not related to phishing activities nor violate our terms of service. For example: • Reviews • Adult content • Illegal content
Dark web	All threats
S3 bucket Amazon	All buckets types
Line platform	All types
Douyin platform	All types
Kumu platform	All types
Fccid.io	All types
xdocs.p	All types
Pastehub	All types

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/