








On-demand service: *Integrated Takedown*

SOCRadar Digital Risk Protection Platform's **Integrated Takedown module** is designed to act rapidly and minimize the impact of threat actors on your brand's reputation or cyber security posture by utilizing its worldwide contact network to request removal.

Takedown categories

-  **Fraudulent domain**
Any domain name which was or is used to commit fraud.
-  **Phishing page**
Any webpage on a domain/subdomain used to steal information by tricking into believing you're on a legitimate website.
-  **Pharming IP**
A fake or alternate IP address where a rogue, corrupted DNS server can direct network traffic.
-  **Fake mobile app**
Any mobile app that mimic the look and/or functionality of legitimate applications to trick unsuspecting users.
-  **Impersonating social account**
A fake or alternate IP address where a rogue, corrupted DNS server can direct network traffic.
-  **Brand abuse***
Increasingly popular form of cyber crime which result in misleading customers or spreading fake news.
-  **Malware infrastructure**
Command & control servers, IP addresses, DNS servers which are known to be utilized by a malware.

* Brand abuse submissions require an official letter of authorization.

One-click initiation and status tracking

Upon detection, confirmation and one-click request on the SOCRadar Portal, the takedown process is immediately taking a start on your behalf to block access to the target malicious infrastructural element as soon as possible. You can track the progress status of the takedown request by accessing your SOCRadar portal.

Utilizing effective global network

SOCRadar Analysts reach out to a variety of providers and reputation networks including Name Server Operators (DNS), Domain Name Registrars, Local CERT Teams, Open Source Threat Sharing Platforms and Browsers' Safe Browsing Teams through email, phone calls or API. Throughout the takedown process, you will receive regular incident updates and notification until the illegitimate content is successfully taken offline.

Procedural experience

SOCRadar's Takedown Team is considering several aspects while initiating takedown process from the geographical region where the illegitimate content is hosted to the type of evidence for submission to speed up the takedown process. Many countries have laws that tend to make internet service providers (ISPs) proactively react to online fraud while others don't.

When fraudulent or phishing domains are concerned, as a reputable vendor, creating the collaboration channels between multiple parties is often a key. SOCRadar has extensive experience and familiarity with how ISPs, hosting providers, Computer Security Incident Response Teams, and Computer Emergency Response Team (CSIRTs, CERTs) handle these cases which helps us provide global-level takedown services.

Reach us now!

Our security analysts are standing by to offer information or help with your purchase.



8609 Westwood Center Dr.
Vienna, VA 22182 USA
+1 (571) 249-4598

info@socradar.io

www.socradar.io



4.9 OUT OF 5 STARS
IN 7 REVIEWS
★★★★★ AS OF 06/2020

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence – all automated and supported by a global team of qualified intelligence analysts – provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.