Recorded Future®

Using Brand Intelligence to Defend Your Organization

Rapidly Detect and Take Down Brand Attacks

Organizations too often are blindsided by cyber attacks targeting their brand. Typosquat websites, leaked data, and command-and-control attacks are all examples of how threat actors are able to attack your brand without ever touching your network. The repercussions can be devastating — ranging from customer distrust to massive financial losses. Security professionals have limited visibility outside of their own organizations' network, and zero visibility into the nefarious corners of the web where cybercriminals are known to launch these attacks. You're dealing with:

PHISHING ATTACKS AGAINST YOUR CUSTOMERS AND EMPLOYEES

Threat actors create typosquat websites to trick customers and employees into disclosing sensitive information via phishing attacks. Without a way to track these sites, security teams spend significant time and resources finding and removing malicious content — often with limited success. Since typosquatting is so difficult to find and take down, many sites remain on the web for extended periods of time, compounding the damage.

LIMITED VISIBILITY LEADS TO MISSED THREATS

Without access to closed and dark web sources, organizations miss vital intelligence about elevated risk to their brand or infrastructure. The most common cyber attacks are initiated on dark and closed web sources, as well as social media. With no clear visibility into these sources, security teams can't identify upcoming attacks and are left scrambling to respond once the attacks are already underway.

DATA LEAKAGE AND THEFT

Stolen corporate data regularly ends up on paste sites and dark web channels. Cybercriminals often purchase leaked credentials from these sources in hopes of gaining a foothold into organizations. While there, they are also able to buy bank information, PII, gift cards, emails, and more. Additionally, employees mistakenly — and all too frequently — upload sensitive company information on sites like GitHub. Unable to monitor for sensitive information on their own, organizations are left exposed to financial, legal, and reputational consequences.

Recorded Future: Unprecedented Brand Intelligence

Recorded Future automatically collects, aggregates, and analyzes data from an unrivaled range of sources spanning the open, closed, deep, and dark web to surface relevant intelligence in real time. Dynamic brand intelligence at scale empowers security teams to proactively detect and take down malicious brand attacks like copycat domains, phishing , data leaks, and more.

Recorded Future's patented algorithm process and natural language processing identifies relationships between emerging threats, your brands, and your infrastructure to deliver easy-to-consume brand intelligence. More than simply monitoring keywords, dynamic brand intelligence enables you to proactively detect brand attacks as they surface and take them down before they damage your business. Recorded Future makes it easy to protect your brand with five primary use cases:

DOMAIN ABUSE DETECTION

Recorded Future automatically collects and analyzes newly registered domains to identify potential typosquat websites and phishing lures. Security teams receive real-time alerts on these threats to their brand using robust pattern search and DNS name permutation detection capabilities. Each domain is assigned a risk score, and live DNS lookups enable deeper investigation into the associated IP address, mail server, and name server. Recorded Future dynamic risk scores are delivered with unprecedented context so you can pivot and dig deeper into associated IPs and domains. Security teams are able to report and initiate a takedown request for domain abuse directly within the platform:

RECORDED FUTURE IN ACTION.

Set up alerts in the Intelligence Goals Library for typosquat detection. Be alerted via email or push the alert into your SIEM. Easily pivot into Intelligence Cards™ for additional information on the malicious domain. Submit a takedown request directly in Recorded Future. The website is quickly removed within an SLA window, mitigating risk and reputational damage.

DATA LEAKAGE MONITORING

Manually searching for leaked company data and credentials on paste sites and the dark web is next to impossible — and dangerous. Recorded Future instantly processes information across these sites — including criminal forums that sell sensitive data. Some domains require specialized access through Insikt Group, Recorded Future's team of world-class analysts, linguists, and security researchers with extensive industry experience. Their expert research and insider access — matched with Recorded Future's broad sourcing and natural language processing — produces instant alerting when there is a data leak. Recorded Future caches these posts, enabling analysts to review and escalate appropriately.

RECORDED FUTURE IN ACTION.

Set up alerts in the Intelligence Goals Library to flag mentions of sensitive corporate data on the web. Be alerted via email or the Recorded Future mobile app when this alert triggers. Review details to learn that proprietary source code was posted by an employee on a paste site like GitHub. Review the copy to verify the incident and submit a takedown request directly in Recorded Future.

INDUSTRY THREAT MONITORING

If cybercriminals are targeting your peer organizations, it is likely that they will be knocking on your door next. Recorded Future surfaces known and emerging threats to your industry in a comprehensive industry threat view, enabling you to proactively defend against risks that threaten your brand and infrastructure. The view is driven by tailored watchlists of your industries and your peers — ensuring that you are getting the brand intelligence you need, and nothing that you don't.

RECORDED FUTURE IN ACTION.

Configure your industry threat view with custom watchlists. Set up alerts for threats targeting your industry. Be alerted via email or the Recorded Future mobile app when a particular malware is targeting other companies in your industry. Review the malware Intelligence Card™ and read an Insikt Note informing you that the malware is being distributed through a technology vulnerability. Share this intelligence with your IT team to prioritize patching the vulnerability.

BRAND ATTACK MITIGATION

Organizations spend significant resources using inefficient and manual tactics to monitor their brand across a limited number of sources. However, closed criminal-access forums, social media channels, and foreign language sites are the real breeding ground for threat actors' ploys. Recorded Future instantly detects and alerts you when your brand is mentioned in reference to a cyber attack, enabling you to take steps to mitigate the attack.

RECORDED FUTURE IN ACTION.

Set up alerts in the Intelligence Goals Library to flag brand mentions with cyber entities. Be alerted via email or the Recorded Future mobile app when this alert triggers. Review the cached copy of the mention to learn about a coordinated phishing attack targeting your customers. Initiate a takedown request directly in Recorded Future.

INFRASTRUCTURE RISK MONITORING

By configuring Recorded Future's technology to continuously monitor for threats against your infrastructure, security teams are able to proactively prevent attacks that could have otherwise launched undetected. With configurable alerts around your domains and IP addresses, teams are instantly alerted when there are malicious mentions of their digital assets. Armed with real-time brand intelligence, security teams are empowered to swiftly secure their network to prevent attacks.

RECORDED FUTURE IN ACTION.

Set up alerts in the Intelligence Goals Library for increased infrastructure risk. Be alerted via email or the Recorded Future mobile app when your IP address has an elevated risk score. Review the risk rules evidence to learn that the IP address has been linked to a command-and-control server. Deactivate the infected computer to prevent damage. Identify associated domains hosted by the same IP address and initiate a takedown request directly in Recorded Future.

Recorded Future's Brand Intelligence Module provides security teams unmatched visibility into threats that were previously difficult or impossible to identify. Collecting from an unrivaled quantity and variety of open, closed, and technical sources, Recorded Future arms security teams with the information and context they need to proactively defend their brand against cyber attacks. Takedown services go the last mile to simplify and expedite the removal of malicious content from the internet.

Key Features

- Unprecedented source coverage spanning an unrivaled quantity and variety of open, technical, closed, deep, and dark web sources
- Machine-scale collection and analysis at the speed and scale of the internet
- Dynamic risk scores and evidence for fast, confident response
- Takedown services to rapidly take down malicious domains
- Configurable, out-of-the-box brand alerts with data visualization capabilities
- Tailored industry-based threat views

Key Benefits

IDC has found that Recorded Future empowers organizations to:

- Identify threats 10x faster
- Identify 22% more threats before impact

www.recordedfuture.com
@RecordedFuture

About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.