

Using Threat Intelligence to Disrupt Adversaries

The Most Comprehensive View of Your Threat Landscape

Whether you're investigating threats in your environment or emerging attack methods on the dark web, you're probably spending too much time manually collecting, analyzing, and piecing together disparate data points into actionable intelligence. You're dealing with:

DATA OVERLOAD

Manually collecting, correlating, and analyzing threat-related data points from multiple systems to derive potential impact is overwhelming for even the most seasoned security analyst. Manual research consumes analyst's valuable time and usually leads to static, incomplete insights.

ANALYSIS PARALYSIS

Successful threat intelligence programs rely on the ability to quickly detect and validate threats. However, most analysts don't have the time to manually investigate each suspicious indicator they come across. This leads to incomplete analysis and missed threats — leaving organizations at risk and often unaware of critical and emerging threats.

COMMUNICATION BREAKDOWN

Too frequently, threat analysts work in silos. There's no simple, efficient way to share real-time assessments and insights with other teams. This leads to ineffective collaboration, duplicated efforts, and wasted time. Security teams need a better, more dynamic way to share relevant intelligence that drives faster response times and more informed decision-making to reduce risk.

DEAD ENDS ON THE DARK WEB

Sites on the deep, dark, and closed web are rich sources of intelligence, but monitoring and collecting from these sources is time-consuming and dangerous — not to mention, many of these sources are incredibly difficult to access. Analysts invest valuable time searching for information, only to find incomplete pieces of what they need, resulting in slower responses to critical threats.

Recorded Future: Unprecedented Threat Intelligence

By collecting information from an unrivaled quantity and variety of open, dark web, and technical sources, Recorded Future eliminates manual research and surfaces intelligence in real time. This provides organizations with a dynamic and comprehensive view of their threat landscape. Without manual tasks weighing them down, analysts are empowered to focus on the high-value work for which they were trained.

Combining a patented algorithm process with world-class human analysis, Recorded Future fuses together billions of entities and delivers original research to dynamically categorize, link, and analyze intelligence with unprecedented speed. This delivers easy-to-consume insights that easily integrate into your existing security tools and workflows to support four primary threat intelligence use cases:

ADVANCED THREAT RESEARCH AND REPORTING

Recorded Future's patented algorithm process and natural language processing technology automatically collects and analyzes data from an unrivaled range of sources in all languages. High-speed, automated analysis, coupled with expert insights from Recorded Future's world-class research group, seamlessly integrate into analysts' threat research workflows — providing a single-pane-of-glass view on each threat actor or indicator of compromise. Dynamic risk scores and rich context support analysts to rapidly assess current risk. Meanwhile, advanced search, real-time alerting, and data visualization capabilities surface the most relevant intelligence to support research and report-writing. Security teams are able to burst analysis siloes by sharing their insights and assessments with the entire enterprise through analyst notes.

RECORDED FUTURE IN ACTION.

Search in Recorded Future for expert analysis on threats relevant to your industry, create visuals of the intelligence, review related Intelligence Cards™, and dig deeper with advanced queries. In addition to producing your threat reporting, create analyst notes within the Recorded Future Security Intelligence Platform, enabling the wider security team to easily access your analysis and insights for more confident, informed decision-making going forward.

ADVANCED DETECTION AND VALIDATION

Recorded Future's machine-scale collection and analysis connects data points from the open and dark web and technical sources. This provides critical context on adversaries, malware, and traffic of interest. Recorded Future's Intelligence Cards™ centralize all known information about a threat actor or indicator in a single place — empowering analysts to respond smarter and faster to incidents. Additionally, threat hunting packages enable organizations to harness advanced analytics and easily implement them into their network, endpoint, or malware security solutions to hunt for threats existing in their environment via YARA and SNORT scripts.

RECORDED FUTURE IN ACTION.

Implement a Recorded Future Threat Hunting Package on a threat actor, like APT33, in your endpoint solution for ongoing, real-time correlation and monitoring of that threat actor's TTPs in your environment. When unusual activity is detected, get immediate alerts and context to accelerate incident response.

DARK WEB INVESTIGATIONS

Having the time, expertise, and resources to manually collect, analyze, and combine intelligence from the dark web is next to impossible. Recorded Future instantly collects and processes intelligence from dark web sources, including hacker, criminal, and extremist forums — some of which are invitation-only and analyzed by Recorded Future's Insikt Group. This expert analyst team is comprised of world-class analysts, linguists, and security researchers with deep government experience, extensive industry expertise, and native foreign language skills. Their research — matched with Recorded Future's broad sourcing and natural language processing capabilities — produces comprehensive, real-time, and actionable security intelligence for confident decision-making.

RECORDED FUTURE IN ACTION.

Use the advanced query builder to search for new exploit kits on select dark web forums. Set up an alert based on the query to be alerted via email or the Recorded Future mobile app when the alert triggers. Easily pivot into Intelligence Cards™ for additional information about the exploit kit before flagging to the wider security team.

Defending against new and emerging attacks requires timely, relevant insights updated in real time. Recorded Future's patented algorithm process combined with world-class human analysis arms analysts with elite threat intelligence and a comprehensive view of their threat landscape to disrupt adversaries and rapidly reduce risk.

Key Features

- Expansive cyber repository with over 1 billion intelligence cards (and growing)
- Unprecedented source coverage spanning an unrivaled quantity and variety of technical, open, closed, deep, and dark web sources
- Automated, machine-scale collection and world-class analysis for real-time security intelligence
- Advanced search capabilities for tailored investigations
- Dynamic risk scores and context for confident decision-making and response
- Access to high-confidence finished intelligence, including malware rules and threat hunting packages from Recorded Future's expert research group.

Key Benefits

IDC found that Recorded Future empowers organizations to:

- Identify threats 10x faster
- Identify 22% more threats before impact
- Reduce time spent compiling reports by 34%
- Boost overall security team efficiency by 32%



 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.