

Threat Intelligence Module

Identify, investigate,
and prioritize cyber threats

Challenge

With more than 2,200 cyber attacks¹ occurring each day, organizations struggle to search, identify, prioritize, and mitigate threats to protect their critical assets and reduce risk.

Solution

Get relevant, real-time insights with Recorded Future's Threat Intelligence Module, which provides a comprehensive view of your unique threat landscape through a combination of automated analytics, finished intelligence, and advanced search and analysis capabilities. The world's most advanced Intelligence Cloud provides increased visibility into threat actors' infrastructure; tactics, techniques, and procedures (TTP); and targets, making it easy to proactively tune controls to reduce risk. And it helps you quickly complete investigations to reduce downtime, reputational damage, and costs.



Key Benefits

- Identify and prioritize threats relevant to your organization.
- Detect and respond to threats faster.
- Get unmatched visibility into closed web sources including dark web ransomware extortion sites.
- Maximize investment in existing security tools.

Key Use Cases

- Access data visualizations to gain more context and identify trends from your threat landscape.
- Use pre-built threat hunting packages, malware hunting and malware alerts with natural language processing, Auto YARA rules, sandbox results, ransomware risk profiles, a victimology table, and more to protect your organization's assets.
- Automate analysis and production of intelligence with Recorded Future AI, expanding your scope of analysis and automating intelligence reports based on your unique threat landscape.
- Prioritize action and get comprehensive visibility into the threat landscape by consolidating security events into a single dashboard.

15.9 hrs

average time organizations save per week on alert investigation, triage, and response efforts with Recorded Future

43%

average increase in security team's capacity when using Recorded Future

64%

of users say their team now has a significantly better understanding of their organization's threat landscape by using Recorded Future

Threat Intelligence

Overview Ransomware Risk Profile Threat Actor Map Malware Threat Map TTP MITRE ATT&CK Matrix Malware Intelligence

Layers Threat Actor Map (+1) Threat Actor Category All Threat Actor All Malware Category All Malware Family All Threat Map Change Last 30 Days + More Reset Export

TTP MITRE ATT&CK Matrix - based on Threat Maps for Acme Corporation

TTPs from your organization's [Method Watch List](#) that have been identified to be in use by your organization's priority actors and/or malware in the last 12 months

Initial Access	1	Initial Access	2	Initial Access	159	Execution	23	Persistence	289	Privilege Escalation	279	Defense Evasion	108	Discovery
External Remote Services T0822	1	Drive-By Compromise T1456	1	Drive-by Compromise T1189	2	User Execution T1204	23	Account Manipulation T1098	33	Account Manipulation T1098	33	Modify Registry T1112	88	System Info Discovery T1082
		Phishing T1660	1	Exploit Public-Facing Application T1190	20	Malicious Link T1204.001	7	Additional Cloud Roles T1098.003	1	Additional Cloud Roles T1098.003	1	Valid Accounts T1078	20	
		External Remote Services T1133			10	Malicious File T1204.002	11	SSH Authorized Keys T1098.004		T1547.001: Registry Run Keys / Startup Folder		Default Accounts 078.001	1	
		Phishing T1566			41			Boot or Logon Autostart Execution T1547		Occurrences in Threat Actor Map	2	Main Accounts 078.002	4	
		Spearphishing Attachment T1586.001			17			Registry Run Keys / Startup Folder T1547.001	78	Registry Run Keys / Startup Folder T1547.001	78	Cloud Accounts T1078.004	1	

Features

Threat Map

Get an automated visual of threat actors and malware relevant to you — across your geography, third parties, industry, and more. See threat trends over time to identify and prioritize threats that matter to you.

NEW

Malware Hunting

Upskill analysts faster with natural language querying capabilities. Dive deep into both static and dynamic malware behaviors without complex queries. And analyze trends and changes in malware over time.²

NEW

Auto YARA rules

Instantly generate detection rules for new and emerging malware, validate them against known good filesets to prevent false positives, and apply them at scale across file systems, email, and downloaded binaries.²

NEW

Malware Alerts

Transform threat hunts from reactive to proactive with real-time alerts. Create, manage, and refine custom detection rules through an intuitive interface, and spot emerging threats before they become problems. Create, manage, and refine custom malware detection rules through a natural language interface. The system watches for what matters to you and flags new variants immediately.²

Enhanced Malware analysis sandbox

See malware in action to understand its impacts. Use a customizable sandbox to detect, observe, and detonate malware in a controlled environment, and get full sandbox report details in the dashboard.²

Advanced Query Builder

Conduct deep targeted searches across Recorded Future's entire intelligence repository.

Custom Alerting

Get notified in real time via email, mobile app, or portal any time a new piece of relevant intelligence is identified.

Threat Hunting Packages

Provide your team with detection mechanisms — including YARA, Snort, and Sigma rules written and tested by Recorded Future's Insikt Group® — to hunt for adversaries, malware, or traffic of interest.

NEW Ransomware Risk Profile

Get an end-to-end view of your ransomware exposure across the attack lifecycle as well as guidance for each threat to identify risks early, prioritize action, and take targeted mitigation steps.

NEW Victimology Table and Intelligence Cards

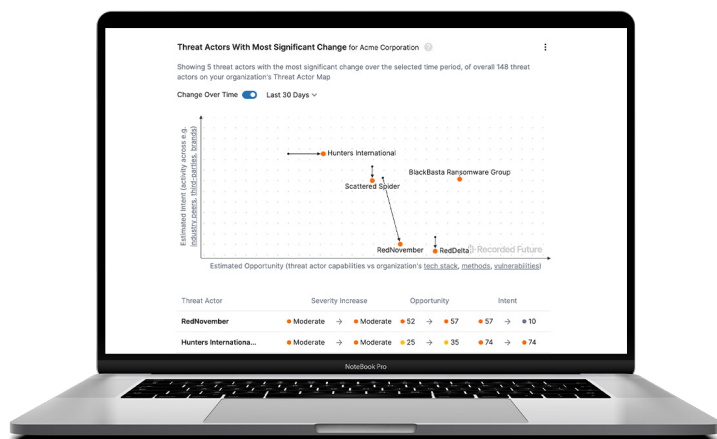
Gain real-time visibility into ransomware victims in your ecosystem, detailed threat actor breakdowns, and secure dark web browsing to help you proactively defend your organization without endangering its risk posture.

NEW AI Reporting

Automatically generate and schedule customized, audience-specific intelligence reports relevant to you, including your threat landscape from a ransomware perspective, saving time and ensuring that leadership and the entire organization stay up to date.

Integrations

Access real-time, machine-readable intelligence in the security technologies you already use with frictionless integrations and a simple API.



See Threat Intelligence Module in action

[Request a demo](#) to learn how to identify, investigate, and mitigate cyber threats with Threat Intelligence.

¹ <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>

² *Malware Intelligence offerings are included in the Recorded Future Threat Intelligence Module. For customers that have requirements exceeding daily usage limits, additional fees may apply.

Recorded Future is the world's largest intelligence company. Recorded Future Precision Intelligence provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries. Learn more at www.recordedfuture.com.