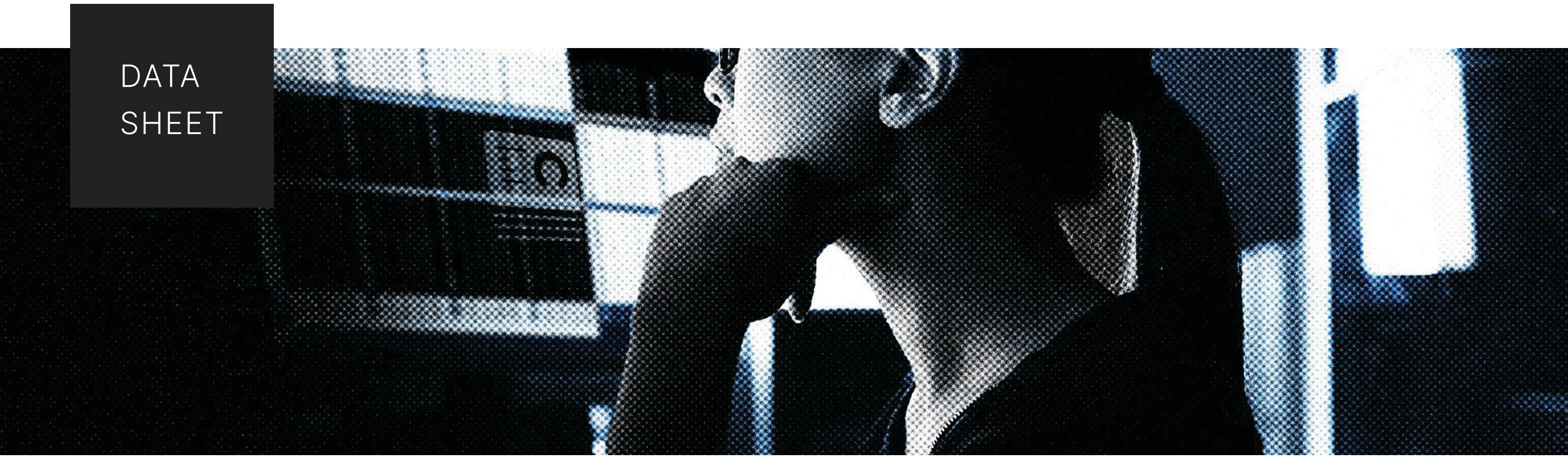
Recorded Future®

DATA SHEET



Threat Intelligence Module

Identify, Investigate, and Prioritize Cyber Threats

Challenge

The modern threat landscape is vast, complex, and constantly evolving. The idea that organizations can be fully secured against any and all potential threats has become untenable. Organizations of all sizes and nearly every industry face a never-ending set of challenges when trying to protect their digital assets from adversaries. The use and implementation of threat intelligence is a critical component of today's modern security team. When used to its full potential, it is often the difference between preventing an incident from happening and being a victim of a cyber incident.

Solution

Defending against new and emerging cyber threats requires timely, relevant insights updated in real-time. Recorded Future's Threat Intelligence module provides a comprehensive view of your unique threat landscape through a combination of automated analytics, human-finished intelligence, and advanced search and analysis capabilities. With our Intelligence Cloud, billions of entities are fused together to deliver original research to dynamically categorize, link, and analyze intelligence with unprecedented speed, arming you with easy-to-consume insights that are easily integrated directly into your existing security tools and workflows.

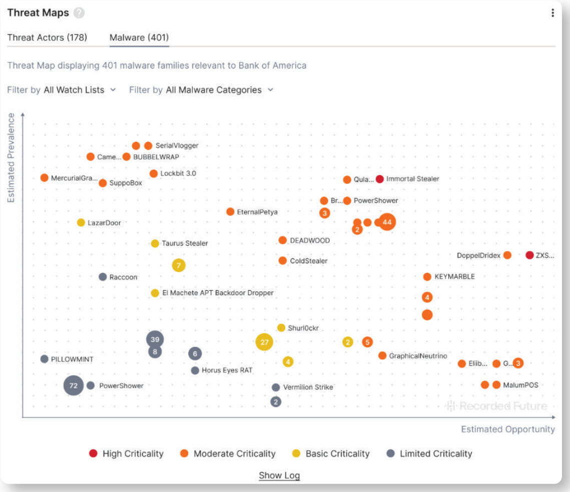
The world's most advanced intelligence cloud empowers you to make fast, confident decisions. Features like advanced querying capabilities, real-time alerting, and threat visualization capabilities provide the context you need for advanced threat research and threat hunting. Quickly detect critical threats with the Recorded Future Threat Intelligence module – and get ahead of emerging ones to disrupt adversaries before they get to you.

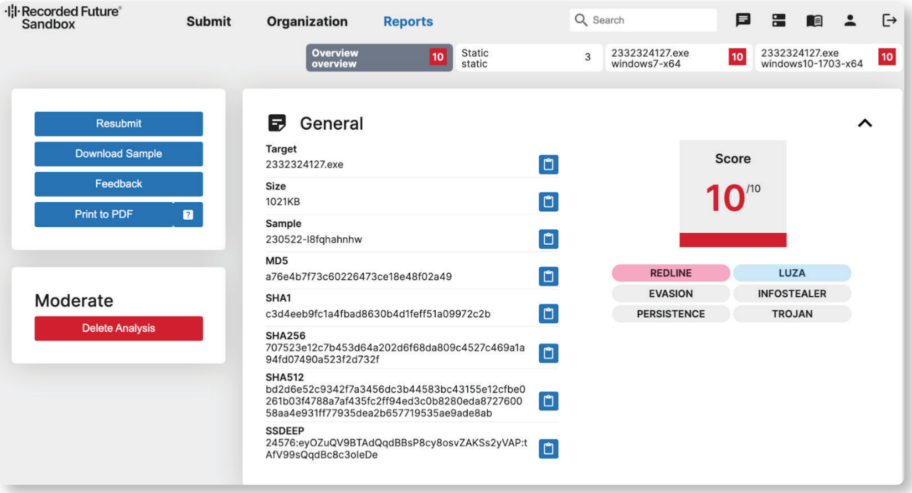
Benefits

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

Key Features

- Threat actor and malware threat maps
- Malware sandbox
- Advanced query builder
- Custom alerting
- Threat hunting packages
- Out-of-the-box integrations





General

Target
2332324127.exe

Size
1021KB

Sample
230522-l8fqhahnhw

MD5
a76e4b7f73c60226473ce18e48f02a49

SHA1
c3d4eeb9fc1a4fbad8630b4d1feff51a09972c2b

SHA256
707523e12c7b453d64a202d6f68da809c4527c469a1a94fd07490a523f2d732f

SHA512
bd2d6e52c9342f7a3456dc3b44583bc43155e12cfbe0261b03f4788a7af435fc2ff94ed3c0b8280eda872760058aa4e931ff77935dea2b657719535ae9ade8ab

SSDEEP
24576:eyOZuQV9BTAdQqdBBsP8cy8osvZAKSs2yVAP:tAfV99sQqdBc8c3oleDe

Score 10/10

Key Features

Feature	Description	In Action
Threat Map	Automated visual of threat actors and malware relevant to you, your third parties, and your industry. See threat trends over time to identify and prioritize threats that matter to you.	A multinational bank's CTI team significantly reduced an influx of alerts, allowing them to concentrate their efforts on the most important, high-priority threat actors. They now focus on the most likely and relevant threats to their organization and industry.
Sandbox	A sandbox solution built with speed and scalability in mind. Automatic ingestion through an API with a fully customizable environment, live control of the detonation, malware tagging, and more to support your investigations and proactive mitigations.	An International Finance company provided numerous outcomes for malware verdicts and malicious phishing domains utilizing the sandbox. In submitting files, they quickly reach a verdict on files as bots or malicious — saving significant time in their investigation. Extracted indicators from the sandbox further help confirm successful malware containment.
Advanced Query Builder	Conduct deep targeted searches across Recorded Future's entire intelligence repository. Save and share searches for easy access to what your team cares about.	Allowed a software company's team to do further research and triage on threat actors for historical data. The team set up specific queries of interest to monitor the dark web for leaked credentials and IOCs of interest.
Custom Alerting	Based on your intelligence requirements, get notified in real-time via email, mobile app, or portal any time a new piece of intelligence is identified.	When alerts identified a client's domain as a mention on a dark web Russian market for leaked credentials, they investigated the alert to find IOCs of interest. They accessed the requisite YARA/Sigma rules to further analyze and mitigate the problem.
Threat Hunting Packages	Provide your team with detection mechanisms, including YARA, Snort, and Sigma rules to hunt for adversaries, malware, or traffic of interest.	Each week a computer hardware company improves its overall security by identifying a trending threat actor and using detection Rules API to pull down relevant YARA/Sigma Rules, then using the hunting packages for threat hunting across their environment.
Integrations	Real-time, machine-readable intelligence in the security technologies you already use with frictionless integrations and a simple API.	A finance company enriches its data with Recorded Future in their SIEM tool to help reduce their time for investigations, specifically for Domain and IP Address reputations, providing more input to the events.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

www.recordedfuture.com @RecordedFuture