

Recorded Future for Resilient

Better incident response with auto-enrichment of IOCs using real-time threat intelligence.

More Context for Better Insight

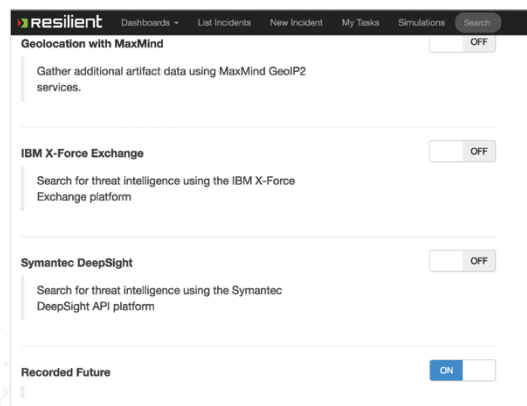
To help organizations proactively defend against attackers, Recorded Future's real-time threat intelligence provides analysts full context of emerging threats from the open, deep, and dark web, including volatile sources. Recorded Future captures and structures this information for security analysis: billions of indexed facts over a multi-year history, linked to sources and authors, and across all languages. We detect reporting of new vulnerabilities, exploits, IOCs (indicators of compromise), exposed company assets, and threat actors targeting organizations and industries. This threat intelligence, tailored to each organization, its IT infrastructure, partners, and industry helps reduce security risk.

Once installed, Recorded Future for Resilient retrieves threat intelligence context and artifacts (including IP addresses, DNS names, and file identity hashes) automatically for artifacts linked to incidents tracked in Resilient.

Adding Enrichment to Incident Artifacts

Recorded Future for Resilient automatically enriches artifacts added to incidents with threat intelligence context. When an incident responder captures an artifact in Resilient, the integration automates a request to Recorded Future for the current threat intelligence enrichment. The enrichment lookup happens as a background task, and the artifact is flagged to the incident responder in Resilient when the enrichment is available. Available enriched artifact types include:

- > net.ip
- > net.name
- > hash.md5
- > hash.sha1
- > hash.fuzzy



Recorded Future for Resilient can be enabled in the Threat Sources Directory in the Administrator Settings



About Resilient

Resilient, an IBM company, provides an Incident Response Platform (IRP) that empowers cyber security teams to transform their security posture. Deployed in more than 100 Fortune 500 and mid-sized enterprises across three continents, Resilient is the industry standard in IR software.

Integration Details

- A deployment of the Resilient IRP is required to use Recorded Future for Resilient
- The Recorded Future for Resilient integration is installed into the Resilient Threat Sources Directory
- A subscription to Recorded Future is required to enable the integration

When a new artifact is attached to an incident that Recorded Future has information on, the artifact is automatically added to the Artifacts List with a "caution" symbol denoting a match with threat intelligence, as shown below.

Clicking on the Hash value itself will display the "hit" from Recorded Future, including a risk score, rules triggered that affect the score, reported event hits, and a link to the Recorded Future Intel Card which has even more information, as shown below.

Similar results are seen for IP Addresses...

...and Domains

Lookups to Recorded Future for Resilient incident artifacts are automatically rescanned periodically until the parent incident is closed.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA | © Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners. | 10/16