Recorded Future

resilient an IBM Company

ABOUT RESILIENT

Resilient, an IBM company, provides an incident response platform (IRP) that empowers cybersecurity 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.

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 technical, open, dark web 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

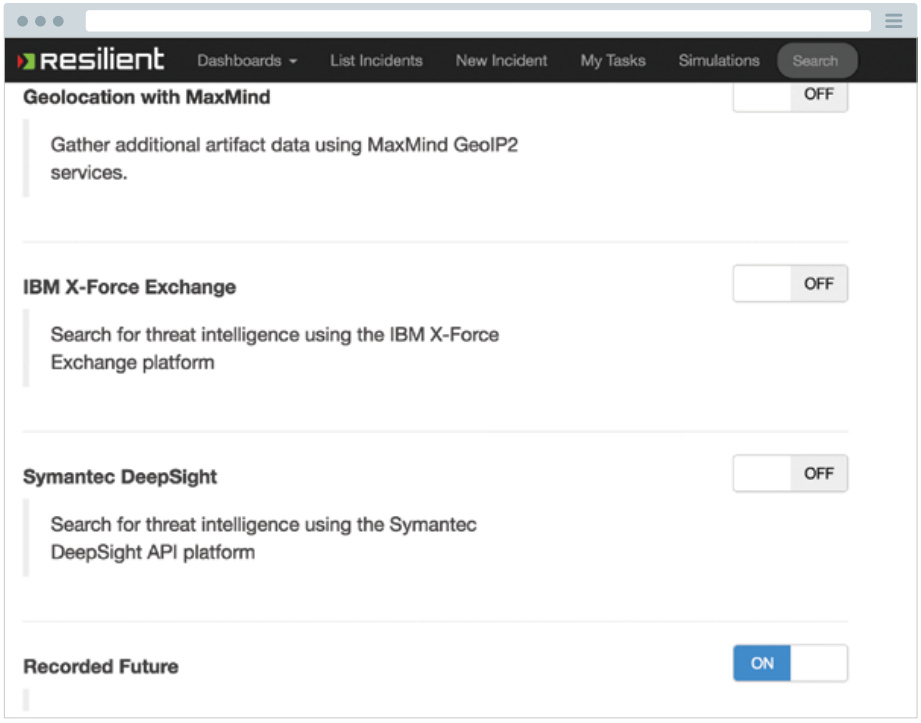
hash.md5

hash.sha1

hash.sha256

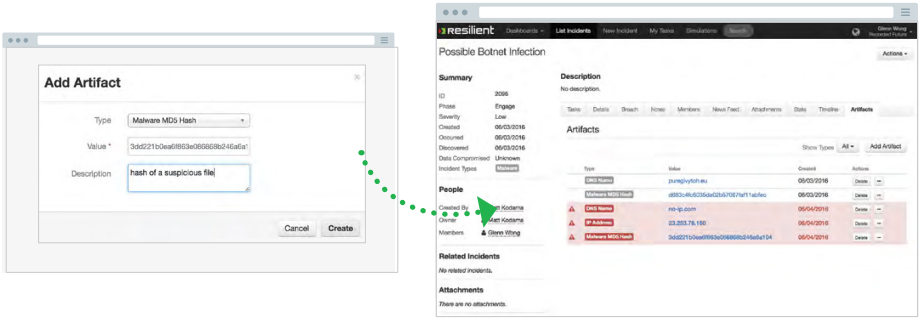
hash.fuzzy

threat.report.cve

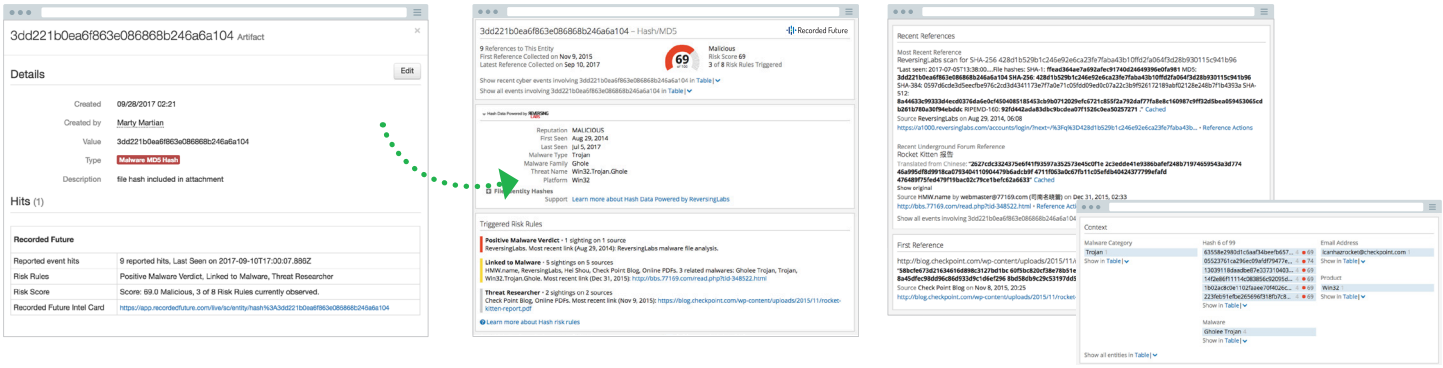


Recorded Future for Resilient can be enabled in the Threat Sources Directory in the Administrator Settings

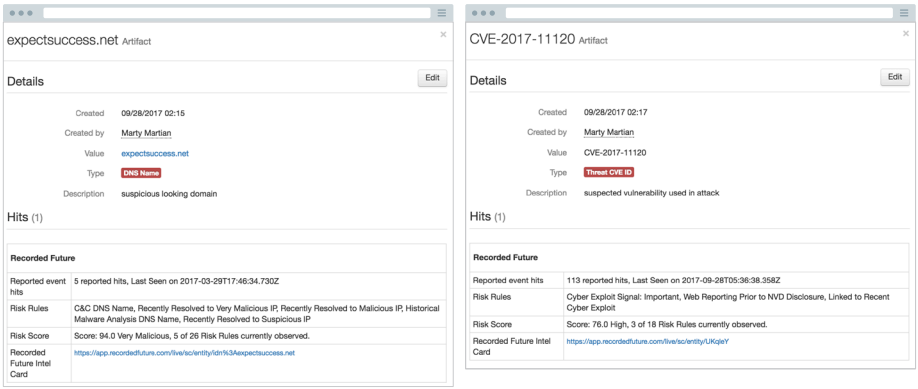
When a new artifact is attached to an incident that Recorded Future has information on, the artifact is automatically added to the Artifacts List with a "caution" symbol denoting a match with threat intelligence, as shown below.



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.

Recorded Future

About Recorded Future

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that’s delivered in real time and packaged for human analysis or instant integration with existing security technology.