Recorded Future

Recorded Future API

The Recorded Future Application Programming Interface (API) provides programmatic access to threat intelligence content and evidence-based risk scores. The API has a straightforward RESTful design with operations for enrichment, monitoring, and correlation. Supported data types include IP addresses, domains and DNS names, file hashes, vulnerabilities, and malware families. The API also has search and lookup operations on entity lists, including threat lists, white lists, and customer-specific watchlists.

Most security teams use this API through packaged integrations with SIEM and incident response platforms, and do not directly develop client code. Advanced security teams use this API to creatively expand on those integrations, or to create specialized threat intelligence integrations with their custom or proprietary security products and workflows.

Use Cases

This API supports three core use cases for automated security integration:

1. Enrichment for incident artifacts, security alerts, and vulnerability scans

Lookup threat intelligence context for a specific observable, indicator of compromise (IOC), vulnerability, or malware family. This rich context includes risk scores and supporting evidence, GEOIP, current threat list inclusions, related threat entities, and recent sightings in highlighted sources such as paste sites, dark web, criminal forums, information security sites, and social media.

2. Monitoring for risks and threats

Search for threat intelligence that meets specific filter criteria (e.g., high risk score, triggered specific risk rules, recently observed) on a customer-defined watchlist. SOC dashboards can display the latest matches for these monitoring searches. Automated scripts can poll and load matches into workflow and ticketing systems.

3. Correlation with logs and alerts

Download current risk lists of IP addresses, hashes, and vulnerabilities for correlation with internal log and alert data, including details and evidence for current risk scores. Correlations are used to automatically raise or lower review priority based on external threat intelligence context. When analysts review an alert or potential incident, correlated threat intelligence context supports fast and accurate verdicts.

Technical Details

Operations

The use cases are supported by four operation types:

1. The lookup operations return enrichment for a single entity. Each API call specifies which enrichment fields to return based on the specific integration requirements.
2. The search operations return a page of entities that meet the specific filter criteria. Each API call specifies filters, sort order, and paging.
3. The risk list operations download a standard risk list in CSV or STIX file format. These risk lists are continuously and automatically updated by Recorded Future.
4. The extension lookup operations return additional enrichment for a single entity, through integrations with our OMNI Intelligence Partners.

These operations are available for six data types as shown in the following table:

Entity Type	Lookup	Extension Lookup	Search	Risk List
Domain	✓	✓	✓	✓
Entity List	✓		✓	
Hash	✓	✓	✓	✓
IP Address	✓	✓	✓	✓
Malware	✓	✓	✓	
Vulnerability	✓	✓	✓	✓

Requests and Responses

Client code calls this API by making REST-style requests. The specific parameters for each API call are encrypted using HTTPS. These API requests may pass through a proxy server in the client network when required.

API responses are sent synchronously. Most responses are data in JSON format. Risk lists are provided as CSV files to simplify integration into SIEMs and similar products. The IP risk list is also available in STIX version 1.1, 1.1.1, and 1.2 formats.

Authentication

API calls are authenticated using tokens, which are specific to an individual user and tied to his/her enterprise deployment. Tokens are specified using HTTP headers and encrypted by HTTPS. Authentication is stateless and is verified for each API call. Hash-based message authentication (HMAC) is supported in addition to the current HTTP header-based authentication.

Licensing

Access to the API is licensed to enterprises with a daily quota of API credits. This daily quota model is used for both pre-packaged and custom integrations. API calls consume a variable number of API credits:

- Each risk list download operation = 5 credits
- Each lookup or search operation which returns results = 1 credit
- Each lookup or search operation which returns only a count = 0 credits

Business warning emails are sent when usage exceeds daily quota. When daily quota is exceeded, API access is automatically disabled for the remainder of that calendar day.

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.

Recorded Future

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution 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 in real time and packaged for human analysis or integration with security technologies.