Recorded Future and EclecticIQ

EclecticIQ Platform is a Threat Intelligence Platform (TIP), enabling organizations to align their defense tactics and strategies with the actual and future threat landscape.

The Recorded Future integration provides both a feed and enricher capabilities. With the feed, users have access to the Recorded Future Risk List which includes IP and file hashes, for example. The results are provided in standard STIX/TAXII protocols including TTPs and Indicators. The enricher allows users to query Domains, hashes, URLs and IP addresses.

INTELLIGENCE AGGREGATION - CENTRAL REPOSITORY FOR THREAT INTELLIGENCE

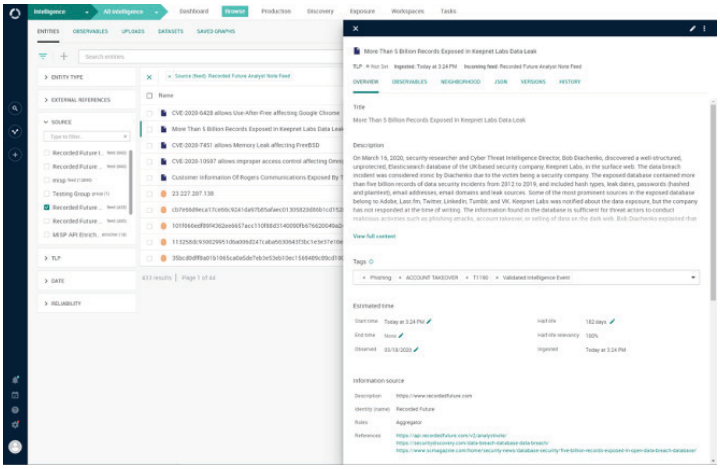
A central knowledgebase ensures the ability to act and align effectively against the latest cyber threats in a timely fashion. Aggregating threat intelligence in a single point of truth keeps the most accurate and up to date record of insights and enrichments from different sources of intelligence including collaboration among security teams and enrichments from internal systems.

EclecticIQ Platform aggregates intelligence from multiple sources, supporting open standards like STIX and a wide range of intelligence integrations. EclecticIQ Platform has a scalable ingestion and automation engine to normalize, correlate, enrich and qualify intelligence at scale.

INGESTION OF INTELLIGENCE FEEDS (ANALYST NOTE, RISK LISTS, ETC.), CONTAINING INDICATORS, URLS, DOMAINS AND HASHES, RELATED RISK RULES

Recorded Future Intelligence Feeds provide a stream of timely reports with their associated, indicator, observables, Risk Rules, and malware entities.

Screenshots below are focused on the Analyst Note Feed. These Feeds are ingested within the EclecticIQ Platform and made available to CTI Analysts for correlation, threat hunting, incident response, investigations and reporting.



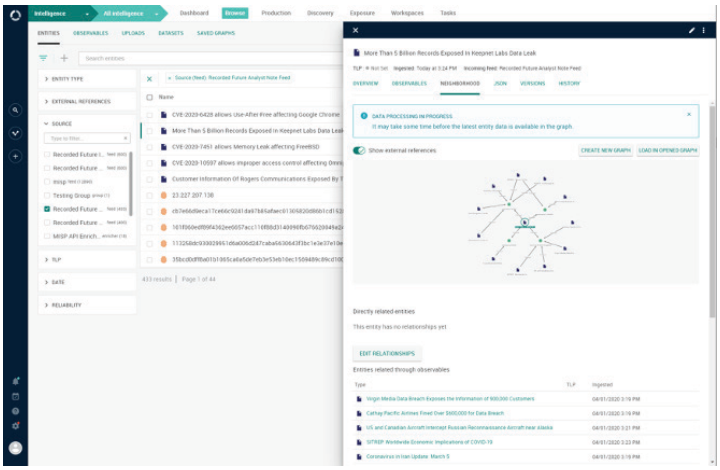
The Integration supports the following endpoints as feeds:

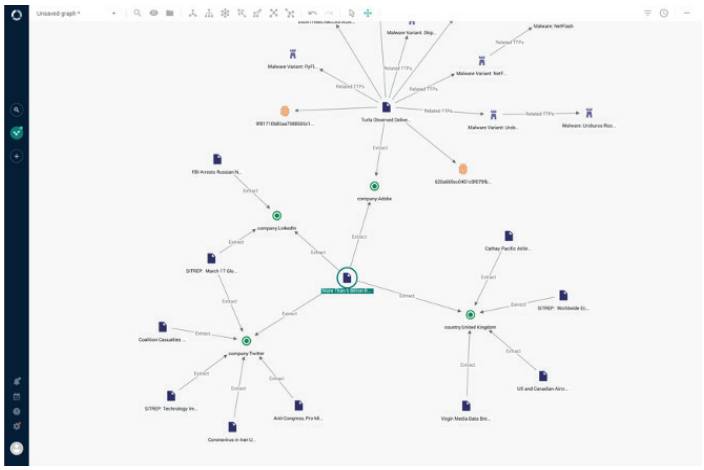
- Analyst Note Feed
- Domain, Hash, IP, URLs, and Vulnerability Feeds

The Integration supports the following observable types as enricher:

- ipv4, domain, hash-md5, hash-sha1, hash-sha256, hash-sha512, uri

DATA SHEET

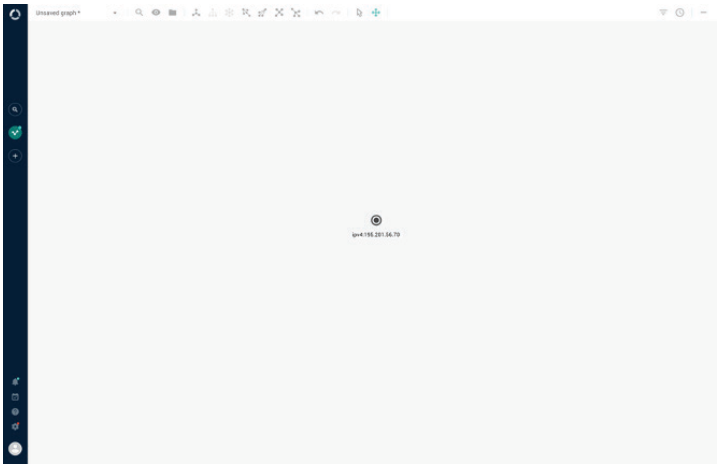


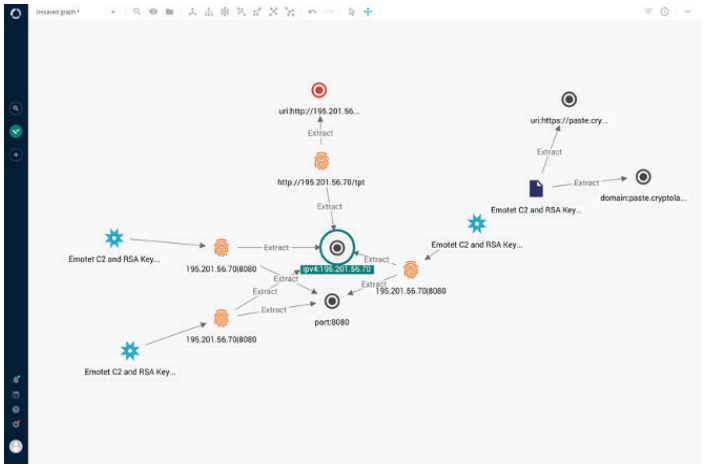


ENRICHMENT OF OBSERVABLES / INDICATORS OF COMPROMISE (IOC)

EclecticIQ Platform Users are able to enrich supported Observable types against the Recorded Future API, allowing to find additional information and context around this data point. For example, the enricher will CTI Analysts to find related malware variants and observables. These observables allow for more path walking opportunities on the platform.

WE COULD PROVIDE MORE EXAMPLES ON FEEDS, UPON REQUEST





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.

www.recordedfuture.com @RecordedFuture

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.

EclecticIQ

About EclecticIQ

EclecticIQ enables intelligence-powered cybersecurity for government organizations and commercial enterprises. We develop analyst-centric products and services that align clients' cybersecurity focus with their threat reality.

facebook.com/eclecticiq @EclecticIQ