EclecticIQ Platform release notes

Product release notes and information

Last generated: April 03, 2017

Last generated on Apr 3, 2017

Table of contents

EclecticIQ Platform release notes 1.14.1

Summary: Release 1.14.1 — Spotlight: interoperability between EclecticIQ Platform instances, out-of-the-box support for Farsight Passive DNS and FireEye Threatscape Report enrichers, and for Cisco AMP Threat Grid Curated Feed and FireEye Threatscape Report incoming feeds.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.1
Release date	2017-04-03

Highlights

This EclecticIQ Platform hotfix release addresses one or more specific issues. For further details about the fixes, see What's new and Fixed bugs.

We did not only fix bugs 🐞, though: we also added a couple of cool new features and we just could not wait for the next standard product release, so we packed them in this hotfix release (*9025*).

EclecticIQ Platform ships with three new data ingestion sources out of the box : **Cisco AMP Threat Grid Curated Feed**, **Farsight Passive DNS**, and **FireEye Threatscape Report**.

Cisco AMP Threat Grid Curated Feed is implemented as an incoming feed. It provides a wealth of curated information about banking Trojans, network streams, suspicious IP addresses, domain names, and DNS entries.

Farsight Passive DNS is implemented as an enricher to feed the platform additional context as suspicious domain names and IP addresses.
The Farsight Passive DNS enricher performs passive DNS lookup, and it returns domain names associated to an IP netblock, or IP addresses associated to a domain name. Enriched data is saved as observables. The context the enricher provides helps to map domain names to IP addresses over time, and to correlate domain names using the same suspicious name server infrastructure.

FireEye Threatscape Report is implemented as an incoming feed and as an enricher to and fetch intelligence reports related to the specified indicators of compromise. Matching reports are ingested as STIX.
The reports provide more context to better understand the threats represented by the indicators of compromise.

Besides email attachments, the IMAP email fetcher incoming feed can now ingest also email body content. When you choose to ingest email body content, it is saved as a report whose title is the email subject, the description is the email body text, and the estimated threat start time is the email sent date.

Last but not least, two or more EclecticIQ Platform instances can talk to each other. Interoperability across platform instances enables you to exchange intelligence and route it to other components of the system more efficiently.

Upgrade to the latest release

- Follow the standard upgrade procedure.

What's new

- Cisco AMP Threat Grid Curated Feed incoming feed (*9023*)
- Farsight Passive DNS enricher for passive DNS lookup (*7484*, *10200*)
- FireEye Threatscape Report incoming feed and enricher to fetch intelligence reports matching specific indicators of compromise (*9030*, *10242*, *10447*)
- Interoperability between EclecticIQ Platform instances: different instances of the platform can now communicate by exchanging data in JSON and STIX formats (*9811*, *9815*, *9818*. *10087*, *10139*)

What's changed

Enhancements

Feeds

- Outgoing feeds performance improvements (*10337*)
- Implemented STIX 1.2 support for the **Cisco AMP Threat Grid Curated Feed** and **Cisco AMP Threat Grid Sample Feed API** incoming feeds (*9023*, *10332*)
- The **IMAP email fetcher** incoming feed can ingest email body content, besides email attachments. It is now possible to select if the feed should ingest email attachments or the email body content. Ingested email body content is saved as a report (*10115*, *10445*)

- The UI of the execution scheduling section of feeds has been simplified to make it user-friendlier (*9911*)

System

- Improved SQL performance (*10291*)
- Improved memory management when creating content in outgoing feeds (*10207*)

Fixed bugs

Enrichers

- **Max low confidence threat score** and **Min high confidence threat score** in the Cisco AMP Threat Grid enricher are mandatory input fields, but they were not marked as such in the UI (*9522*)
- It would not be possible to save user-created extract queries in the Elastic Sightings enricher (*10498*)
- Addressed some issues affecting the VirusTotal enricher (*9925*, *10073*, *10088*, *10126*)
- Addressed some issues affecting the Elastic Sightings enricher (*10009*)

Entities

- Occasionally, it would not be possible to open entities with a large number of relationships (in the order of magnitude of several tens of thousands) (*9056*)

Feeds

- Outgoing feeds: **Verify SSL** option was added to the TAXII inbox transport type (*9810*)
- Outgoing feeds: when using the TAXII inbox transport type with TAXII 1.0, it is not possible to select a destination collection because TAXII 1.0 does not support collection selection (*9897*, *10191*)
- Outgoing and incoming feeds: when using the TAXII inbox transport type with STIX 1.2 as the content type to exchange data between two platform instances, the incoming feed may not be able to process the incoming data correctly (*9902*)
- Incoming feeds: addressed an issue that would occasionally cause Threat Grid incoming feed requests to time out (*10147*)

Misc

- Addressed a PDF ingestion issue (*9978*)
- Addressed an issue concerning the update of blob IDs after ID ref resolution (*10067*)

Rules

- Addressed an issue concerning regex processing in extract rules (*9903*)

Upload

- Occasionally, a successful PDF upload would not result in a successful content creation (*10504*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Apr 3, 2017