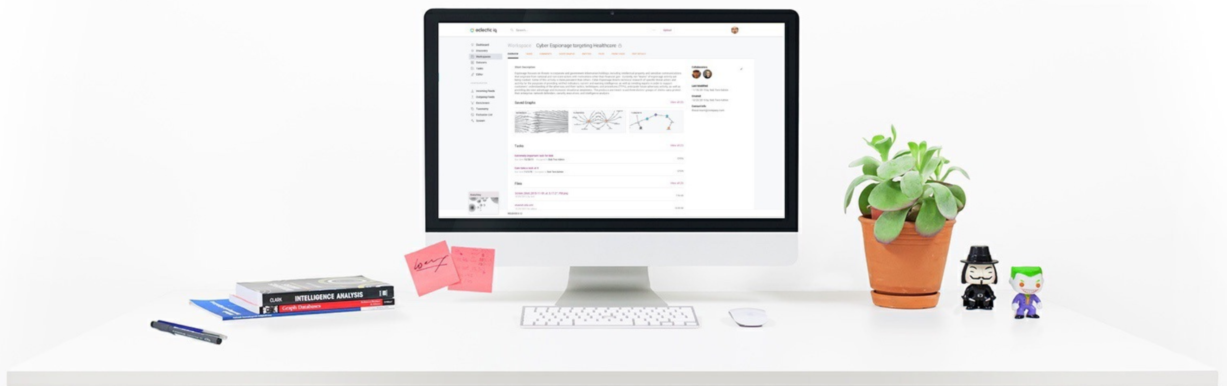
EclecticIQ Platform release notes

Product release notes and information

Last generated: December 31, 2016



Last generated on Dec 31, 2016

Table of Contents

EclecticIQ Platform release notes 1.14.0

Summary: Release 1.14.0 — Spotlight: autosave your work, undo and redo actions on the graph, build custom enricher extensions, get intel from the new PassiveTotal enrichers.

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

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.0
Release date	2016-12-31

Highlights

Winter tastes like orange and cinnamon. EclecticIQ Platform release 1.14.0 tastes like autosave, undo/redo to your heart's content, and BYOE (Build Your Own Enrichers).

When working with data, these are possibly the worst user scenarios ever:

- The Death Star blows up the planet you're working from.
- You lose unsaved work.

We're gathering intelligence to address the former issue, but we got you covered right now from the risk of losing unsaved work: autosave saves the day and your data.

Autosave

Autosave automatically saves a copy of your work in progess, be it a graph view, a taxonomy entry, an entity, and so on, in case you are about to be logged out because of a session timeout, or if connection to the host server(s) is lost unexpectedly.
Context-sensitive pop-up dialog windows inform you about the issue, and notify you about saving your work in progress.

You can resume your work from where you left it as soon as the system becomes available again: upon signing in, a message notifies you about your previously saved work.
If an edit conflict occurs because in the meantime another user has modified the same content, you can decide what to do with one click: you can keep your changes and discard the other user's edits, keep the other user's changes and discard yours, or do what we all know is by far the best thing to do at the end of the day: procrastinate, create a copy of the data and call off the final decision to mañana.

Undo and redo

You can also get sloppier and get away with it, too: unleash the power of oops! Well, at least as long as you're in the graph, thanks to the new *undo/redo* feature. On the graph you can undo the last action, as well as redo the previously undone action. Very handy, especially when examining scenarios with complex relationships.

Autorefresh

The graph view *automatically refreshes* when you edit an entity or its extracts: when the graph is open, an entity is loaded on the graph canvas, and you edit the entity or its extracts on the corresponding detail pane, the graph view is updated to reflect the changes.

Configure session timeout

The web-base UI features a new section where you can *configure the user session timeout interval*. To access this option, go to **System > Server > General/Server settings > Edit settings**.

Observables

Entity extracts + enrichment extracts = Observables

Entity extracts and enrichments/enrichment extracts now live together on one tab called **Observables** in the entity detail pane. This UI change features a cleaner layout, and it is your one-stop-shop to clearly examine all the observable elements related to an entity, regardless their source being the entity or external enrichment data. You can filter the observables listed on this tab by origin — entity extracts, enrichment process extracts, or manually added by users — as well as based on other criteria like maliciousness or specific observable data types.

Enrichers

We added *new enrichers* to help you draw an accurate picture of the threat scenario under investigation, where you can clearly see the tree and the forest. The new PassiveTotal enrichers augment entities with extra context to help you cross-reference domain names vs IP addresses, retrieve whois details, and look up geolocation information.

Besides the built-in, ready-to-use enrichers that ship with the platform, you can *create your own custom enricher extensions*. We provide a boilerplate that you can use as a scaffold to build your custom enricher, and documentation to cover the tricky parts. Just kidding, there are no tricky parts. But the doc is there, just in case.

Help

On a closing note: EclecticIQ Platform ships with *built-in help*. Who knew? That’s why we moved the help link outside the user profile drop-down menu and turned it into a **(?)** icon on the header bar next to the notification icon and the avatar picture.

Upgrade to the latest release

- Follow the standard upgrade procedure.

What’s new

Features and functionality

Discovery

- You can now edit an existing discovery rule, and then click **Save and Re-Run for All Time** to run it again and discover all relevant entities *since the beginning of time*; that is, all discovered entities, not only those added since the previous successful execution of the same rule (*8336*)

Enrichers

- Four new enrichers are available to poll data from. The data generates meaningful extracts that augment entity intel value and relevance:
  - The PassiveTotal **Passive DNS** `(https://api.passivetotal.org/api/docs/#api-dns)` enricher returns extracts containing cross-reference information about domain names and the IP addresses they refer to (*8378*)
  - The PassiveTotal **Get WHOIS** `(https://api.passivetotal.org/api/docs/#api-whois)` enricher returns extracts containing cross-reference information about domain names and the individuals or entities who own them (*8379*)
  - The PassiveTotal **IP/Domain** `(https://api.passivetotal.org/api/docs/#api-enrichment-getv2enrichmentquery)` enricher returns extracts containing geolocation information about IP addresses (*8380*)
  - The PassiveTotal **Malware** `(https://api.passivetotal.org/api/docs/#api-enrichment-getv2enrichmentmalwarequery)` enricher returns extracts containing malware information related to the queried host or domain (*8381*)

Extracts

- You can remove a specific occurrence of an extract from the entity it is related to, when the extract occurrence is no longer relevant (*8108*)

Graph

- Undo the last action and redo the previously undone action (*6355*)

Groups

- The group detail pane has a new **Users** tab that shows the group members. You can filter users, as well as act on them by selecting the desired options from the context menus (*8504*)

Observables

- You can create and add new observables to entities from the **Observables** tab in the entity detail pane (*8184*)
- On the **Observables** tab in the entity detail pane you can see the number of connections an observable has to other entities (*8604*)
- On the **Observables** tab in the entity detail pane you can filter observables by level 1 or 2 to reduce unwanted noise and to focus only on the relevant observables (*8781*)

System

- It is possible to configure the user session timeout interval in the UI through **System > Server > General/Server settings > Edit settings** (*8590*, *8591*)
- If the connection to the API is lost, the current screen locks and a message is displayed while the platform automatically attempts to reconnect (*8592*)
- The RPM packages to install EclecticIQ Platform and its components are available also for CentOS 6.5, besides CentOS 7 (*8173*, *8550*)

Documentation

- Documentation is now available also as PDF (*7676*, *8371*, *8372*)

New

- Rules in the getting started documentation
- How to work with the PassiveTotal enrichers in the *How to* section
- Build custom enricher extensions to implement ad-hoc integrations
- Integrations with external systems and services:
  - Cisco AMP OpenDNS integration
  - Cisco AMP Threat Grid integration
  - Flashpoint integration
  - Intel 471 integration
  - PassiveTotal integration
  - Splunk integration
  - VirusTotal integration
- Hardware requirements for system administrators in the *RPM installation and configuration* guide

Updated

- Discovery in the *Getting started* guide
- Configure the enricher section in *How to work with the Elasticsearch sightings enricher*
- How to install the platform via an RPM package, the shorter how-to version of the *RPM installation and configuration* guide
- RPM installation and configuration guide
- Reindex Elasticsearch in the *Bootstrap* and *Upgrade* sections of the *RPM installation and configuration* guide

What's changed

Enhancements

Discovery

- Improved handling of deleted discovery rules (*8616*)

Enrichers

- Fixtures for enrichers now include a preset source reliability value, which users can modify at any moment (*8518*)

Entities

- During entity ingestion, any entity raw attachments, such as embedded CybOX objects or embedded images, undergo a deduplication check (*8095*)
- Entity extracts are now called *observables*. You can view any observables related to an entity on the **Observables** tab in the entity detail pane. (*8415*, *8447*)

Graph

- On the graph, the **Layout** menu was redesigned to make it more efficient and user-friendly (*6377*)
- On the graph, an **(i)** icon is displayed next to the **Layouts** menu header: hover the mouse over it or click it to view a short explanation of the available graph layout formats (*8756*)
- The graph view refreshes when you edit an entity or its extracts: when the graph is open, an entity is loaded on the graph canvas, and you edit the entity or its extracts on the corresponding detail pane, the graph view is updated to reflect the changes (*7941*)
- Graph ingestion of observables was improved (*8762*)
- We upgraded KeyLine from version 2.11 to version 3.2. This introduces a number of improvements to the graph, including extensive control over the time bar events, more granular control of node hierarchy, and WebGL as the default API for WebGL-enabled browsers (*6522*)

Ingestion

- In case a connection problem or an error occurs, pending payload data is sent to a queue, so that its ingestion can be resumed as soon as the system is available again (*8757*)

Processes

- We added a nightly build step to our CI cycle to improve, among others, QA and testing processes (*6059*)

Rules

- Entity extract rules were refactored to improve processing speed (*8217*)

System

- Implemented support for gzip-compressed HTTP responses in Cabby (*8492*)
- Improved management of Elasticsearch index mapping during migrations, for example, to upgrade to a newer platform release (*8239*)
- Improved management of task runs with no task object (*7780*)

UI

- A dialog window is displayed to notify users when the current session is about to expire. User work in progress is automatically saved. A notification confirming that your work was saved is displayed on the login screen as well (*7693*, *8276*, *8589*, *8624*, *8758*, *8760*)
- When a user changes their password, a notification is displayed to notify them about the successful or failed outcome of the action (*8678*)
- **Enrich** and **Run now** actions, previously available as clickable buttons on the detail panes of incoming/outgoing feeds and discovery rules, are now incorporated as menu options in the **Actions** menu (*8586*)

- The built-in help menu option was moved outside the user avatar drop-down menu. Now it is a clickable **(?)** icon on the header bar next to the notification icon and the avatar profile picture (*8400*, *8465*, *8503*, *8508*)
- Improved behavior of filter menus to provide a more consistent and predictable user experience across the platform GUI (*8585*)
- Pagination can remember a user’s page size selection (*8567*)
- Whitespace is correctly preserved in the entity descriptions of incoming entities (*8611*)
- The **Exposure** feature was refactored to improve modularity (*6762*)
- The UI areas providing information and control over incoming and outgoing feeds were refactored to improve usability (*8750*)
- UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*8427*)

Deprecated

N/A

Fixed bugs

Entities

- When creating a TTP entity including CAPEC information, an unnecessary dot character (“.”) would be visible on the entity detail pane (*8252*)
- Deleting an entity through the **Actions > Delete** menu option on the entity detail pane would leave the detail pane open, instead of automatically closing it (*8253*)
- When creating an incident entity including **Impact** characteristics, user-entered data would not be saved correctly (*8538*)
- A sighting with an empty security control characteristic section would still produce a security control observable related to the entity (*8895*)

Entity builder

- The **Targeted victim** form on the CIQ editor would not correctly check for required fields (*8459*)

Feeds

- Occasionally, an outgoing feed task may hang after correctly completing a run (*8593*)
- An output feed using the **EIQ Extracts CSV** output content type would not automatically flag exported entities as **Detection**, **Prevention**, or **Sighting** in **Exposure**, even if the outgoing feed in question is associated to one of these options (*8282*)
- Content update strategy options in outgoing feeds using the same dataset(s) as source and whose content type is set to **EclecticIQ Extracts CSV** would not always yield consistent results (*9000*)

Graph

- Occasionally, grouping elements on the graph would fail; at each subsequent click, numbers displayed on the graph would double (*8142*)
- Occasionally, grouping elements on the graph would produce unexpected results (*8643*)
- Occasionally, loading entities containing special characters in the name would fail (*8605*)
- Occasionally, loading entities onto the graph would produce unnamed, undefined relationship elements (*8556*)
- When changing the visibility of a workspace from private to public, a graph pinned to the workspace before the visibility change would not be available anymore (*8226*)

Observables

- It would not be possible to delete an observable obtained through enrichment (*8573*)

Rules

- Occasionally, when creating a new entity rule the rule may fail to execute (*8587*)
- Occasionally, creating or editing an entity or an extract rule would fail (*8751*, *8872*)
- Rule content criteria would not always produce the expected results (*8883*, *8929*)

System

- It would not be possible to restart PostgreSQL and automatically start autorecovering it without first restarting also the *platform-api* service and Celery workers (*8271*)
- Fixed a JavaScript compatibility issue in IE 11 concerning multiple definitions of a property in strict mode (*8690*)

UI

- Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*7534*, *7766*, *7846*, *8012*, *8317*, *8327*, *8328*, *8349*, *8392*, *8428*, *8430*, *8450*, *8457*, *8461*, *8497*, *8502*, *8519*, *8534*, *8539*, *8540*, *8541*, *8545*, *8549*, *8551*, *8597*, *8601*, *8603*, *8610*, *8623*, *8653*, *8654*, *8666*, *8669*, *8680*, *8686*, *8687*, *8691*, *8754*, *8768*, *8774*, *8775*, *8799*, *8808*, *8820*, *8823*, *8827*, *8844*, *8847*, *8860*, *8861*, *8866*, *8873*, *8875*, *8877*, *8878*, *8884*, *8886*, *8887*, *8889*, *8890*, *8891*, *8915*, *8928*, *8934*, *8935*, *8939*, *8940*, *8969*, *8971*, *8979*, *8980*, *8982*, *8984*, *8986*, *8994*, *8997*)

Upload

- Occasionally, it would not be possible to manually upload a PDF or an XML file (*8596*)

Workspaces

- It would not be possible to change a workspace from private to public using the lock icon on the workspace header (*9004*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

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

Last generated on Dec 31, 2016