EclecticIQ Platform release notes

Product release notes and information

Last generated: October 20, 2017

Table of contents

EclecticIQ Platform release notes 2.0 (Yay!)

Release 2.0 — Spotlight: a brand new UI redesigned from scratch with context-aware navigation; IOC-centric analysis with observables; enhanced intel reporting, out-of-the-box support for CIRCL, CVE and Shodan enrichers; AWS S3 and CVE incoming feeds, CAPEC support.

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	2.0
Release date	2017-10-02

Highlights

Version 2.0! We changed the whole first digit in our versioning system, and since we were at it we threw in a platform release sporting a completely redesigned UI. Plus a ton of new features and improvements under the hood to make it easier and more intuitive to add data sources, analyze ingested information, and share it with fellow analysts and other parties. (*5624*)

Revamped UI 2.0

The *new UI* aims at improving navigation and discoverability, while keeping you focused on the data that matters to you:

- The dashboard is more intuitive. It offers a structured overview of the available platform intel, and any pending user tasks.
  Not happy with the layout? Click ✎ on the top-left corner to rearrange the widgets as you please.

- Context-aware navigation makes it easier to find your way inside the platform, and it keeps clicking as limited as possible:
  - The left-hand navigation sidebar enables you to search for and create entities, access workspaces and user tasks, as well as your user profile and the system settings.
  - The top navigation bar keeps things neat and organized by grouping options under two main groups:
    - **Intelligence** keeps you focused on intel analysis and collaboration.

      Within **Intelligence**, you can select **All intelligence**, or you can directly jump to the **All workspaces** overview to select a workspace where you or your team organize and structure a specific platform intel subset.
    - **Data configuration** lets you configure data sources, data dissemination channels, as well as the business rules to manage intel acquisition and distribution as needed.
  - Redesigned, user-friendlier quick filters ( ) allow highlighting and isolating specific clusters of information to zero in on during an analysis.

IOC-centric analysis with observables

Remember when Pluto was demoted, and then reinstated as a dwarf planet ? We felt the same about observables. Analysts can now use *observables* to perform IOC-centric and incident-centric analysis:

- Observables behave like standalone items: you can add and ingest observables as distinct items, besides adding them to the entities they are related to.
- The observable **Link name** field enables you to label observable relationships: depending on the parent entity they are related to, observables can take predefined **Link name** values that define the relationships between observables and their parent entities. These labels add context, and they help understand the role of an observable relative to the parent entity it refers to.

  For example, an observable can represent a vulnerability, a targeted victim, a malicious piece of infrastructure, and so on. It can be observed outside the organization, or sighted within the organization.

  This additional information enables analysts assess the intelligence value and the relevance of observables, which makes triaging easier.
- The observable detail pane, similar to the entity detail pane, provides a clear view of the observable details, its relationships with other observables, and the neighboring threat landscape.
- On the entity detail pane, **Observables** tab, you can show or hide the new tree structure view to inspect observable relationships with entities and with other observables in an intuitive way.
- On the entity and the observable detail pane, **Observables** tab, you can directly go to an observable external data source.
  Clicking the link to an external resource on the **Observables** tab opens the target on a new tab.
- Since observables are indexed you can browse, search for, and find observables.

> If you upgrade the platform from a previous version, rewire observables to make them platform 2.0-compliant.

Enhanced intel reporting

A new *rich text editor* enables threat analysts to author *intelligence reports* easily and efficiently, and to distribute them through outgoing feeds:

- The intel report editor guides analysts in the report writing process, so that they can leverage platform intelligence without leaving the editor.
- They can then publish the entire intel report or only a report digest in HTML format through outgoing feeds.

Command palette (beta)

Click stress? No worries, we got you covered. Ditch the mouse and browse through commands like a ninja with the **Command palette**:

- Press **CTRL + SHIFT + P** to display the **Command palette**.
- Press ↑ **Pg up** or ↓ **Pg dn** to scroll through the platform commands.
  Alternatively, press **TAB** or **SHIFT + TAB**.
- The command palette includes search with autocomplete: start typing a command name to get a result list with commands containing your typed input.
- To select a command, select it, and then press **ENTER**, or click it.
  For example, manually add a new observable.
- Press **ESC** to close the **Command palette**.

More new features and new user guide

Among the new goodies we added to this release:

- You get notified when enrichers are automatically disabled. For example, this can happen with open source data sources enforcing caps and limits, or when requests repeatedly time out. The notification message prompts you to re-enable the enricher, so that it can resume normal operation.
- New enrichers and incoming feeds to poll data from CIRCL and Shodan.

The documentation has changed:

- A new **User guide** replaces the previous *Getting started* guide, as well as most user-targeted how-to articles.
  This is part of an ongoing effort to consolidate and simplify documentation to make it user-friendlier.

- We are gradually moving to a continuous documentation delivery approach:
  - From this release, the documentation package is decoupled from the platform installation packages.
    You can download the documentation package separately from the same location the platform install packages are available from, and install it separately.
  - The documentation is going to be updated more often than the platform. You may want to check the standard platform download location from time to time to download the latest doc package.
  - The documentation versioning format is *<platform_version>-<documentation_version>*.
    Example: *2.0.1-1*

The platform documentation is shipped together with the platform installation packages. When you install or upgrade the platform, the documentation is included in the process.

However, you may occasionally wish to install the documentation separately. For example, to update to a more recent version of the help.

To install the platform documentation on *CentOS* and *RHEL*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ yum install -y eclecticiq-platform-docs-{version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ yum install -y eclecticiq-platform-docs-2.0.1-1

# Install the latest version of the documentation
$ yum install -y eclecticiq-platform-docs
```

To install the platform documentation on *Ubuntu Server*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ apt-get install -y eclecticiq-platform-docs-{version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ apt-get install -y eclecticiq-platform-docs-2.0.1-1

# Install the latest version of the documentation
$ apt-get install -y eclecticiq-platform-docs
```

The default install location for the platform documentation is */opt/eclecticiq/platform/docs*.

For a more detailed list of changes, enhancements and new features, refer to the sections below.

Upgrade to the latest release

Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

Before upgrading, make sure you back up core data such as platform configuration files and databases, familiarize with the upgrade procedure, migrate the PostgreSQL database and reindex Elasticsearch, and run a final check to verify that the upgrade completed successfully.

Rewire observables to v.2.0

> Rewiring observables to v.2.0 is a one-off task you need to perform only when upgrading EclecticIQ Platform from v.1.14.x to 2.0.

After successfully upgrading EclecticIQ Platform from version 1.14.x to 2.0, you need to run `eiq-platform observable refresh`.

Run this script only after booting up the platform, and after starting all platform components. The platform needs to be fully up and running for the observable refresh script to work correctly.

From v.2.0 observables are powerful tools to drive IOC-centric analysis. Observables ingested and created with previous versions of the platform need to be rewired and upgraded to v.2.0, so that the platform can, among others, index them and make them searchable.

The script reparses existing observables to update their format to platform 2.0-compliant.

Run the script from the terminal or the command line:

```
$ export EIQ_PLATFORM_SETTINGS=/opt/eclecticiq/etc/eclecticiq/platform_settings.py
$ /opt/eclecticiq/platform/api/bin/eiq-platform observable refresh --workers=4
```

`workers`

It is a mandatory parameter.
It takes an integer as a value.
If you do not specify any value, it defaults to `1`.

It defines the number of workers the script should concurrently run in parallel.
The process is resource-intensive, and it takes some time to complete: gauge the number of workers based on your system resources.
`4` workers is a rule-of-thumb value to run the script with a limited impact on normal platform operation.

Logging

- After initializing, the script starts discovering items to process, and outputting log information to the terminal.
- After successfully completing, it notifies you with the following message: `all entities processed`.

Errors

- If the user terminates the script before it completes, the script returns `Aborted!`.
- If an error occurs during execution, the script returns `an unexpected worker error occurred`, along with traceback information.

In case of errors, you may want to check the traceback information, as well as the `first_entity_id` and `last_entity_id` values in the log block preceding the error message: they correspond to the first and last entities in the last successfully processed batch before the error.

Example:

```
{"event": "sending batch to search", "first_entity_id": "00209576-bd04-48be-a4f0-c9a865b2b0c0",
"last_entity_id": "0024eceb-fb14-44ee-8e8d-6dad0ce58849", "level": "info", "logger":
"eiq.platform.scripts.bulk_refresh_extracts", "timestamp": "2017-09-01T16:26:44.685313Z",
"worker_pid": 9332}
```

What's new

Enrichers

- **CIRCL** enricher to retrieve all the IP addresses associated with the input SSL certificate `hash-sha1` fingerprints (*12188*)
- **CIRCL** enricher to retrieve all the domain names associated with the input SSL certificate `hash-sha1` fingerprints (*12188*)
- **CVE** enricher to retrieve information about common software and hardware vulnerabilities, along with the corresponding exposures, based on the input **`cve`** `(https://cve.mitre.org/cve/identifiers/)` observables (*10455*)
- The **Shodan** enricher takes a wealth of input observable types to help you discover which of your devices are connected to the Internet, where they are located, and who is using them (*12257*)
- You get notified when an enricher is automatically disabled. Click the enricher name on the notification message to go to the corresponding configuration page, where you can re-enable the enricher (*10107*, *10108*)
- An enrichment option is added to the observable context menu (*13169*)
- Enrichments show notifications displaying the status of an ongoing job (*13026*)

Feeds

- **CAPEC XML** is a new incoming feed content type to retrieve **Common Attack Pattern Enumeration and Classification (CAPEC)** `(https://capec.mitre.org/)` information. Ingested data is processed and saved as **TTP entities** `(https://stixproject.github.io/data-model/1.2/ttp/ttptype/)`
  The STIX ID is based on the CAPEC ID — the default naming convention of a stanbdard CAPEC-ingested TTP starts with the *[CAPEC-<numeric reference>]* prefix — and it is idempotent across uploads (*10460*)
- **CVE Search API** is a new incoming feed transport type to retrieve complete CVE (Common Vulnerability and Exposures) records from the CVE database hosted by CIRCL (Computer Incident Response Center Luxembourg). CVE information is ingested as a STIX package containing an exploit target (*10455*, *10620*)
- MISP to EclecticIQ Platform data mapping schemas as a preparatory step to supporting MISP ingestion into the platform (*11681*)
- The **OpenPhish** and the **PhishMe Intelligence** incoming feeds enable you to ingest phishing URLs and richer phishing intelligence
- **S3** is a supported transport mechanism for incoming and outgoing feeds, so that you can store and retrieve data to and from AWS S3 (*12075*)

Observables

- You can now search for observables in the same way as you search for entities (*8812*)
- Observables feature a detail pane, just like entities, where you can review related observables, as well as neighborhood relationships (*8445*)

UI

- The **Command palette** enables you to scroll through and to select platform commands using the keyboard (*9500*)
- Quick filters are more intuitive and easier to use to perform quick searches on the fly (*8964*)
- A new horizontal navigation bar enables you to make multiple selections, and to apply bulk actions to the selected items in search results, on dataset views, on entities detail panes, and on observable detail panes (*8961*)
- When your user session is about to expire, you get notified, and your work is automatically saved.
  When your user session expires, you get notified, and you are prompted to sing in again (*7693*)

- You are notified if an incorrect value is entered in the platform (*12670*)
- A graph can be exported as an image (*13008*)

What's changed

Enhancements

Observables

- The information displayed for enrichment observables now incldues the source extract for an enrichment observable — for example, the source IP address of a domain name observable — and the date of the most recent enrichment for that observable (*8824*)

UI

- Enter UI v.2.0 (*5624*)
- TLP options and captions are consistent throughout the UI (*10601*)

Fixed bugs

EclecticIQ Platform 2.0 includes more than a hundred bug fixes to improve stability, robustness, interoperability with external systems and applications both upstream and downstream in the system chain.

UI bug fixes address cosmetic, as well as functional issues, to get rid of known usability hiccups, and to improve consistent behavior across the UI.

The following sections give an overview of selected bug fixes to provide context and scope. The lists are not exhaustive. If you have any questions about a specific bug fix, feel free to contact us at support@eclecticiq.com.

Enrichers

Among the enricher-related issues we fixed:

- Enricher success rate visibility
- Enrichers were erroneously included in the system job overview
- Entity creation could cause enrichers to fail
- `extracts-unique` enricher search index errors
- Missing **Source reliability** default value for enrichers
- PassiveTotal passive DNS enricher not working as expected
- Splunk enricher not working as expected

Entities

Among the entity-related issues we fixed:

- Adding entities to a task

- Creating, editing, and updating entities in the entity editor/entity builder; accessing draft entities in the entity editor/entity builder
- Deleting entities from UI and PostgreSQL
- Downloading entities as original or exporting them as JSON
- Entity rule content criteria inconsistency
- Exposure override settings inconsistency
- Filtering entities by origin
- **Impact** characteristic of incidents not keeping loss estimation value after saving
- Modifying entity and extract rules
- Removing entities from datasets

Graph

Among the graph-related issues we fixed:

- Deleted items persist and are visible on the graph
- Item grouping on the graph
- Item visibility on the graph
- Items loaded and disappearing on the graph
- **Path** visibility on the graph
- Unwanted **Undefined** relationships on the graph

Ingestion and dissemination

Among the ingestion and dissemination-related issues we fixed:

- Deleting feeds
- Entity ingestion hiccups and inconsistencies, occasionally
- Manual file upload for users who do not belong to any group
- Indicators can be removed from datasets while editing (*12641*)
- Content type can be changed in incoming feed after adding a collection (*13106*)

Observables

Among the observable-related issues we fixed:

- Filtering by observable in **Exposure** not working as expected
- Filtering observables
- Manually adding observables to indicators
- Observable rules not working as expected, occasionally
- Opening the observable detail pane when the graph is open
- Removing ignored observables on the active view
- Search action triggered by clicking an observable
- Sorting observables by number of connections

System

Among the system-related issues we fixed:

- Adding a user to a user group from the group detail pane

- Elasticsearch would occasionally hang or crash upon processing badly-formed queries
- Packages are successfully ingested using real data (*13002*)
- Email messages are successfully uploaded to the platform (*12982*)

UI

Among the UI-related issues we fixed:

- Cosmetic and functional issues affecting buttons, icons, menus, missing notifications, auto-discovery, quick filters, item sorting on the active view, user information display on feed views, pagination

Known issues

- Updating an entity may erroneously return a *created new entity* message (*7246*)
- Exposure count inconsistencies before and after sorting (*9595*)
- After editing the title of an entity on the entity detail pane, the change is not reflected in the entity result table (*9673*)
- Audit trail logging may unexpectedly throw errors (*10148*)
- Ingesting very large packages between two platform instances throws a memory error during data serialization (*10152*)
- Deleting entities from PostgreSQL instead of the UI may cause the graph to stop working (*10405*)
- A TLP override value for a feed does not propagate to the entities in the feed (*10529*)
- Memory usage may spike when creating content for outgoing feeds (*10557*)
- When creating a new entity rule, not all applicable data sources may be available for selection (*10925*)
- The **Matches** tab on entity and observable rule detail panes throws and error (*11952*)
- The *back* button on the user management page does not work as expected (*12005*)
- Selecting 100 or more observable, and then creating an indicator from the selected items throws an HTTP 400 error (*12071*)
- Web browser built-in password manager does not prompt users to save the login credentials to access the platform (*12094*)
- Sorting items by maliciousness classification does not work as expected (*12115*)
- UI cosmetic issues when displaying the web-based UI in Firefox and MS Edge (Windows, Mac OS X) (*12401*)
- Time displayed on charts is out of sync with system time (*12440*)
- **Send email** outgoing feed task does not return any error message to users when it fails (*12445*)
- Pagination does not reset correctly after changing the number of items to display per page (*12461*)
- Creating an entity with a POST API call, and then immediately deleting it does not remove it from Elasticsearch (*12485*)
- Proxy password encoding issue (*12521*)
- Cosmetic issue affecting the entity detail pane **Actions** menu (*12556*)
- Missing sort option for entity table columns on incoming and outgoing feeds (*12618*)
- Missing validation on some inpout fields (*12670*)
- Missing user icon to flag user-created observables (*12678*)
- Signin in to the platform may take too long (*12706*)

- Outgoing feed anonymization **Skip paths** group selections do not produce the expected results (*12713*)
- Observable tree structure view does not reflect the actual parent-child relationships of the displayed items (*12732*)
- Usability issue affecting PDF viewing inside the platform (*12737*)
- Editing a manually uploaded entity removes it from the uploaded entity view (*12766*)
- Opening an outdated version of an entity from the version tab in the entity detail pane displays the selected outdated entity in full page instead of inside the detail pane (*12773*)
- Double-clicking an entity in a group of entities with different types displays an empty entity detail pane (*12785*)
- Moving or resizing widgets on the dashboard to rearrange them may occasionally not work as expected; minor cosmetic issues affecting dashboard widgets (*12784*, *12813*, *12837*)

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 Oct 20, 2017