EclecticIQ Platform release notes

Product release notes and information

Last generated: January 12, 2018

Table of contents

EclecticIQ Platform release notes 2.1.0

Release 2.1.0 — Spotlight: an automated platform installation script for CentOS and Ubuntu; an improved public API; a downloadable SDK to facilitate custom extension building; new feature that saves your work and remembers surfed pages in the platform.

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	2.1.0
Release date	2018-01-12

Highlights

Version 2.1! We bring you a ton of platform upgrades with helpful new UI elements. And a ton of new improvements to make the platform easier and more intuitive.

Upgrades

- **Python 3.6 Upgrade** Upgrading all production deployments (Centos, Ubuntu, AMI etc.) to Python 3.6.
- **PostgreSQL 9.6 → 10.x Upgrade** Upgrading all production deployments to PostgreSQL 10. Read https://www.postgresql.org/docs/10/static/release-10-1.html to know more.
- **Elastic Stack 5.6 Upgrade** Upgrading all production deployments to Elastic Stack 5.6. Read https://www.elastic.co/guide/en/elasticsearch/reference/5.6/release-notes-5.6.0.html to know more.
- **Neo4j 3.0 Upgrade** Upgrading all production deployments to Neo4j 3.0 Upgrade. Read https://neo4j.com/release-notes/neo4j-3-0-0/ to know more.

All-in install script

From this release installing the platform is much easier, thanks to the provided documentation-driven install script. Run the script from the command line, and follow the prompts. And if you feel like taking a break for a GTA V or Horizon Zero Dawn game; no sweat, and enjoy it. You can resume the install process at a later time from where you left it. (14235)

What's new

SDK

- Our SDK provides a structured framework to build your extensions, to implement transport and content types for custom feeds, as well as to create new enrichers, based on your organization needs and requirements.

Feeds

- Incoming and outgoing feeds remember the patterns and actions to ease the user journey. (12697)
- You can now run a feed immediately after saving it. (12709)
- **New archive format** - Besides the *.zip* format, manual file upload and incoming feeds support extracting compressed files also from *.rar* archives, with or without password protection.

Observables

- You can now delete extracted and unlinked observables from the platform. (14571, 12278)

UI

- Levels are introduced to help manage log configuration. (5186)
- The platform remembers the state of the pages. (14129)

What's changed

Public API

- Our public API includes a number of endpoints exposing services such as the authentication mechanism, as well as access to the platform assets and resources, such as entities, observables, enrichment tasks, and data sources.

Enhancements

Search

- Search is enhanced for better results (14130)

Observables

- New lists are introduced in the observable **Neighborhood** tab to show how the observable is related to the intelligence in the platform.

Fixed bugs

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.

Feeds

- Mount point download can no longer make requests to internal resources using incoming and outgoing feeds. (14277)
- SFTP incoming feed is working as expected. (14920)
- Maliciousness property for Proofpoint incoming feed is fixed and works as expected. (15088)
- Spycloud enricher, Capec, Crowdstrike indicator feed, and Threat grid curator feed work as expected. (15119, 15120, 15121, 15122)
- CSV schema now contains meta.taxonomy column for both entity-based and extract-based CSV.

Rules

- In Discovery rule modal, packages are renamed to entities for consistency. (14673)

Entities

- To provide clarity, only latest version of related entities is displayed. (14707)

Notifications

- Email notification for workspaces is configurable. (14800)

UI

- Notifications are moved to bottom left of the page, a box pops up notifying you of all the creations, updates, and changes in the platform. You can also look at the bell icon to see all the notifications.

System

Among the system-related issues we fixed:

- Wget installed version is now correct. (14464)

Known issues

- Platform does not work correctly if the workspace module is disabled.
- *Skip* and *Replace* paths isn't working on outgoing feeds for HTML reports.
- UI is slower when you load more than 100 entities on the graph.
- Title change of an entity is not reflected in the result table.
- Filter by source is not working for rules creation.
- Creating an indicator with more than 100 observables returns an error.
- Labels on the graph are not positioned correctly.
- Performance issues with MS Edge and MS Internet Explorer web browsers.
- Adding too many entities to a dataset is slow.
- Hashes are different for same STIX content.
- Manually adding a *Sighting* characteristic to an exposed entity does not affect the *Sighting* attribute of that entity on the *Exposure* view.
- Intel set was renamed to *Datasets*, but the GUI may still display some *intel set* leftovers.
- Entity relation is not displayed in the graph in the *Neighbourhood* tab.
- Filtering is not working for ingestion timestamp.
- Tags only search for exact matches.

Danger:
Due to breaking changes, the following enrichers and incoming feeds are *not working* on EclecticIQ Platform release *1.14.4 (and earlier) until release 2.0.2 included*:

- Enrichers:
  - FireEye iSIGHT
  - Intel 471
  - Recorded Future
- Incoming feeds:
  - BFK API
  - Cisco Threat Grid Curated Feed
  - Cisco Threat Grid Samples API
  - Crowdstrike Falcon Intelligence Indicator Feed
  - Crowdstrike Falcon Intelligence Reports Feed
  - Crowdstrike Falcon Intelligence Threat Actor Feed
  - FireEye iSIGHT Intelligence Report API

To restore full functionality for these enrichers and incoming feeds, upgrade to EclecticIQ Platform release *2.1.0* or later.

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 Jan 12, 2018