EclecticIQ Platform release notes

Product release notes and information

Last generated: July 21, 2017

Table of contents

EclecticIQ Platform release notes 1.14.4

Release 1.14.4 — Spotlight: out-of-the-box support for Crowdstrike as an incoming feed and an enricher, and for BFK as an incoming feed; install on CentOS and RHEL from a TAR archive.

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	1.14.4
Release date	2017-07-21

Highlights

With this release, EclecticIQ Platform extends out-of-the-box support to the following intel providers (*11357*):

- BFK, incoming feed
- Crowdstrike Falcon Intelligence Indicator, incoming feed
- Crowdstrike Falcon Intelligence Indicator, enricher

A new platform installation option is available for CentOS and RHEL OSs:

- Install the plaform from a TAR archive

You can now upgrade the platform also on Ubuntu Server:

- Upgrade the platform from the APT repository

Upgrade to the latest release

- Follow the standard upgrade procedure.

What's new

Feeds

- **BFK** is available as a data source through incoming feeds (*11425*, *11664*)
- **Crowdstrike Falcon Intelligence** is available as a data source through incoming feeds (*11665*)
- **Crowdstrike Falcon Intelligence** is available as a data source through enrichment (*11666*)

- It is now possible to delete or purge an incoming feed (*11388*, *11539*):
  - *Delete the feed* to remove the incoming feed configuration.
    The platform stops ingesting and processing data from the designated data source for the feed.
    Existing data linked to the feed are preserved, such as previously ingested and processed entities and relationships.
  - *Purge the feed* to remove the incoming feed configuration, and any data ingested through or linked to the feed.
    The platform stops ingesting and processing data from the designated data source for the feed.
    Data linked to the feed are completely removed as well, such as entities previously ingested through the feed.

What's changed

Enhancements

Entities

- Indicator wrappers, that is, empty indicators wrapped around CybOX observables whose CybOX `idref`s point to external observables that have not yet been ingested and processed, are ignored and excluded from search and from the graph when the observable `idref`s they contain are successfully resolved to the actual observables they represent (*11630*)

Feeds

- Ingestion improvements in Fox-IT incoming feeds (*11935*)

System

- The default number of workers was raised to 17 for the platform API, and to 4 for OpenTAXII (*11936*)
- Upgrade the platform to a more recent release on Ubuntu Server (*11495*)
- Install the platform on CentOS and RHEL from a TAR archive (*11284*, *11842*, *11869*)
- Improved interoperability with the Postfix email server component (*11500*)
- Improved interoperability with external authentication mechanisms such as LDAP, AD, and SAML (*11812*, *11927*)

UI

- Usability improvements in the scheduler (*10676*)
- When a form detects missing data, an error message is displayed, but the fields with the missing data would not be highlighted to the user (*12047*)

Fixed bugs

Feeds

- The date selector to filter entity display by dates in incoming feeds would not work correctly (*11709*)
- The FireEye iSIGHT Intelligence Report incoming feed would stop working after upgrading the platform (*12182*)

Ingestion and dissemination

- Uploading a password-protected *zip* file to the platform would fail (*11839*)
- Uploading an email body content as *eml* file would fail (*12008*)
- After a non-resolved observable `idref` embedded in a wrapper indicator is resolved to the actual observable it represents, the fully resolved wrapped observable would not always be deleted from Elasticsearch (*12090*)

System

- LDAP users whose user name contains a comma character would not be able to sign in to the platform (*11951*)
- It would not be possible to edit or update the permissions of AD-synced role groups from within the platform (*12138*)

UI

- Fixed several issues to improve usability, as well as look and feel (*11718*, *11789*, *11828*, *11931*, *11950*, *11965*, *11988*, *11991*, *12013*, *12048*, *12092*, *12100*, *12105*, *12107*, *12112*)

Known issues

- Drop-down menus near the header and footer sections are partially covered by the header and footer areas — IE 11 only (*6693*)
- After editing the title of an entity on the entity detail pane, the change is not reflected in the entity result table (*9673*)
- After completing clearing the graph canvas and refreshing the graph page, previsouly deleted entities are displayed again (*12128*)

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 Jul 21, 2017