EclecticIQ

EclecticIQ Platform

Functionality and specifications

Last generated 08/19/2021

Table of contents

EclecticIQ Platform empowers threat analysts to perform faster, better, and deeper investigations while disseminating intelligence at machine-speed.

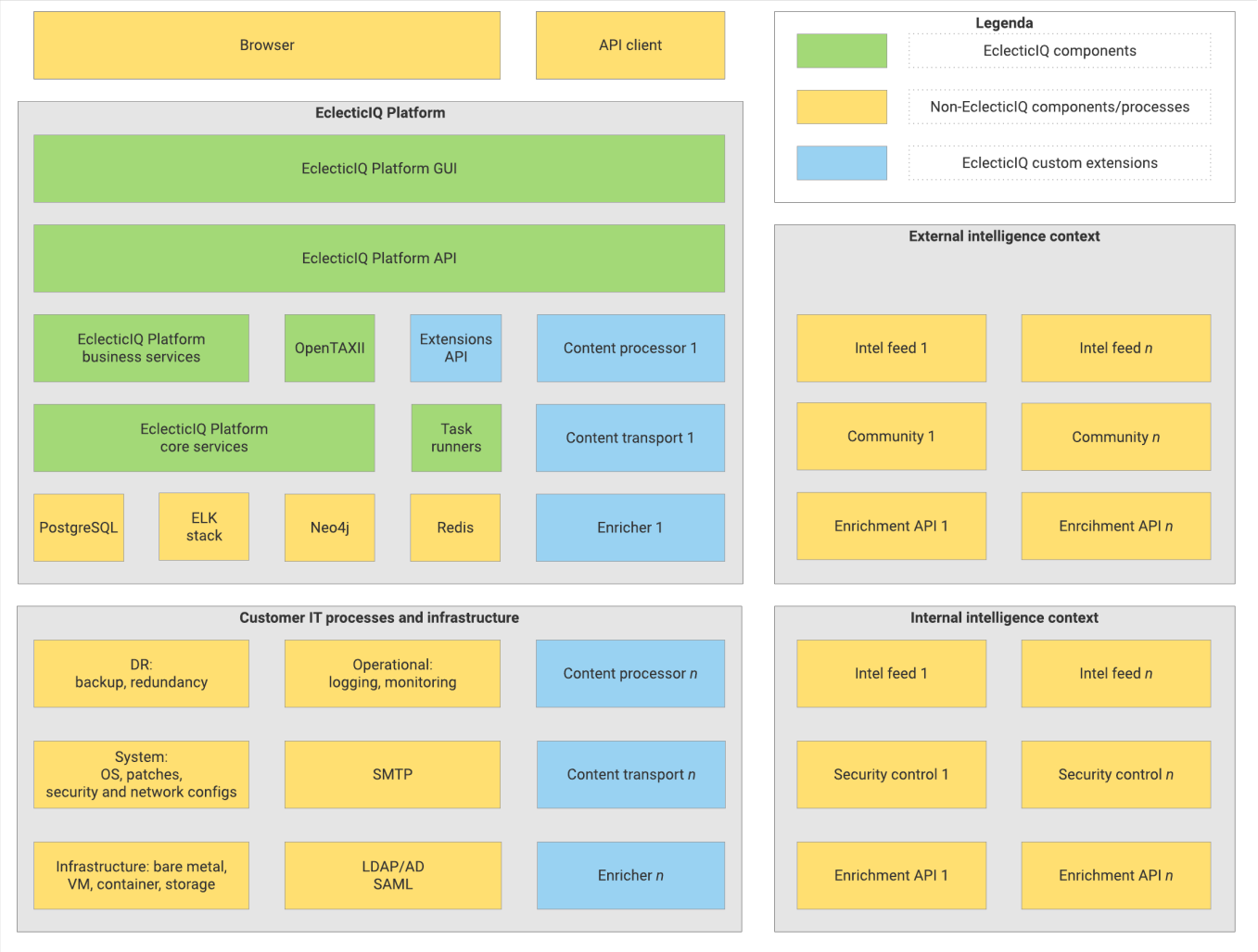
This document presents the technical aspects of EclecticIQ Platform to provide an overview of the system, as well as its key functionality and interface.

Version	2.10.0
Release Date	29 Jun 2021

System overview

Component overview

The following diagran represents a high level architecture of EclecticIQ Platform.



Deployment

Deployment types

Hardware requirements for EclecticIQ Platform can vary, depending on the target system and the environment you plan to install the platform to.

The requirements outlined in this section are general guidelines that work in most cases, but they are not tailored to any specific situation or use case.

Hardware requirements

Hardware requirements for EclecticIQ Platform can vary, depending on the target system and the environment you plan to install the platform to.

The requirements outlined in this section are general guidelines that work in most cases, but they are not tailored to any specific situation or use case.

Hardware requirement guidelines for EclecticIQ Platform and related dependencies installation on a single system/machine.

Hardware	Minimum	Recommended	Notes
CPUs	4	8	Core count includes HT.
CPU speed	2.5 GHz	2.5 GHz or faster	
Memory	32 GB	64 GB or more	• A production environment should feature at least 64 GB memory. Consider increasing the memory to 96 GB when dealing with, for example, large data corpora ingestion or data-intensive graph visualizations. • Redis requires at least 4 GB memory (maxmemory 4gb in /etc/eclecticiq-redis/redis.conf). Consider increasing the memory to 8 GB or more to process very long queues (millions of queued items). • Operations and tasks carried out through the web-based GUI may be memory-intensive. Occasionally, the web browser may use ~1 GB or more. • Monitor system memory usage to determine if your system requires increasing memory to operate smoothly.

Hardware	Minimum	Recommended	Notes
Storage	SATA, 100 IOPS	SSD, 200-500 IOPS	• Local attached storage is preferable to SAN or NAS. Platform operations are write-intensive. • Recommended IOPS range: 200-500.
Drives	5	10	10 drives enable setting up 5 sets of mirrored drives (RAID 1).
Drive sizes (GB)	10, 10, 25, 50, 200	20, 20, 50, 75, 300	Each platform database should be allocated to a dedicated drive for data storage.
Drive allocation (GB)	10	20	Root (EclecticIQ Platform + Redis).
	10	20	Log data storage.
	25	50	Neo4j, graph database.
	100	150	Elasticsearch, searching and indexing. On average, allocate Elasticsearch about half the amount of space you assign to PostgreSQL.
	200	300	PostgreSQL, main data storage.
Network	2 network interfaces	2 network interfaces	One interface for production, the other for system management.
Install size	~240 GB	~240 GB	Full install, based on the VM image size.

Supported OS versions

The following operating systems are supported:

- CentOS 7 latest release – currently CentOS 7.9 (2009)[1]
- Red Hat Enterprise Linux 7 latest release – currently Red Hat Enterprise Linux 7.9[2]

Dependencies

EclecticIQ Platform requires the third-party software listed in this section to operate correctly:

- CentOS and RHEL(see page 0)

CentOS and RHEL

Dependency	Version	Reference
eclecticiq-statsite	4.0.1	Metrics aggregator for the dashboard based on Statsite[3].
elasticsearch-oss	7.9.1	Elasticsearch[4]
jdk	1.8.0	OpenJDK[5] for Elasticsearch.
kibana-oss	7.9.1	Kibana reference documentation[6].
logstash-oss	7.9.1	Logstash reference documentation[7].
neo4j	3.5.12 Community	Neo4j[8]

1 https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7.2009
2 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.9_release_notes/index
3 https://statsite.github.io/statsite/
4 https://www.elastic.co/
5 https://openjdk.java.net/
6 https://www.elastic.co/guide/en/kibana/current/getting-started.html
7 https://www.elastic.co/guide/en/logstash/5.6/index.html
8 http://neo4j.com/

Dependency	Version	Reference
nginx	1.16.1	Nginx[9]
poppler-utils	0.26.5	poppler-utils[10].
postfix	2.10.1	Postfix[11].
postgresql11	11.5	PostgreSQL[12].
python3	3.6.8	Python 3.6.8[13].
redis	5.0.6	Redis[14].
unrar	5.3.0	unrar for creating and extracting .rar archives.
xmlsec1	1.2.20	xmlsec1 for signing, verifying, encrypting, and decrypting XML documents.

Bundled software dependencies

EclecticIQ Platform depends on these software libraries to operate correctly; they are installed along with the platform.

9 https://nginx.org/
10 https://pkgs.org/download/poppler-utils
11 http://www.postfix.org/
12 https://yum.postgresql.org/repopackages.php
13 https://www.python.org/downloads/release/python-368/
14 http://redis.io/

Backend dependencies

```
alembic==1.3.2
amqp==5.0.5               # via kombu
antlr4-python3-runtime==4.8  # via stix2-patterns
apispec-webframeworks==0.5.0
apispec[yaml]==3.3.0
appdirs==1.4.4            # via urlextract
attrs==20.3.0
authlib==0.14.3           # via flask-azure-oauth
backcall==0.2.0           # via ipython
bcrypt==3.1.7             # via paramiko
beautifulsoup4==4.7.1
billiard==3.6.3.0         # via celery
blinker==1.4
boto3==1.4.7
botocore==1.7.48          # via boto3, s3transfer
cabby==0.1.23
cachetools==3.1.0
cairocffi==1.1.0          # via cairosvg, weasyprint
cairosvg==2.5.1           # via weasyprint
cattrs==1.0.0
celery==5.0.5
certifi==2020.4.5.2       # via elasticsearch, elasticsearch-curator, requests
cffi==1.14.0              # via bcrypt, cairocffi, cryptography, pynacl, weasyprint
chardet==4.0.0            # via requests
click-didyoumean==0.0.3   # via celery
click-plugins==1.1.1      # via celery
click-repl==0.1.6         # via celery
click==7.1.2
colorama==0.3.9
colorlog==4.1.0           # via cabby
cryptography==3.4.7
cssselect2==0.3.0         # via cairosvg, weasyprint
datauri==1.0.0
dateparser==0.7.4
decorator==4.4.2          # via ipython, traitlets, validators
defusedxml==0.6.0         # via cairosvg, pysaml2
docutils==0.16            # via botocore
elasticsearch-curator==5.8.3-eiq
elasticsearch==7.9.1
elementpath==2.2.1        # via xmlschema
fancycompleter==0.9.1     # via pdbpp
feedparser==5.2.1
flamegraph==0.1-eiq
flask-azure-oauth==0.5.0
flask-classful==0.14.2
flask-jwt==0.2.0
flask-redis==0.3.0
flask-sqlalchemy==2.4.4
flask==1.1.2
furl==2.0.0
geoip2==2.9.0
gunicorn==20.0.4
```

```
html5lib==1.1             # via weasyprint
idna==2.10                # via requests, urlextract
importlib-metadata==1.7.0  # via kombu
importlib-resources==5.1.2  # via pysaml2
inflect==5.0.2
ipdb==0.11
ipython-genutils==0.2.0   # via traitlets
ipython==7.16.0
iso3166==1.0.1
itsdangerous==1.1.0       # via flask, flask-jwt
jedi==0.17.0              # via ipython
jinja2==2.11.3
jmespath==0.10.0          # via boto3, botocore
jsonlines==1.2.0
jsonschema==3.0.2
kombu==5.0.2
libtaxii==1.1.118         # via cabby, opentaxii
lxml==4.6.3
mako==1.1.3               # via alembic
markupsafe==1.1.1
marshmallow==3.10.0
maxminddb==1.5.4          # via geoip2
mixbox==1.0.3             # via stix-validator
msal==1.7.0
objectivistix==1.2.1
opentaxii==0.2.0
ordered-set==4.0.1        # via mixbox
ordereddict==1.1          # via stix-validator
orderedmultidict==1.0.1   # via furl
paramiko==2.4.2
parso==0.7.0              # via jedi
pdbpp==0.9.5
pexpect==4.8.0            # via ipython
pickleshare==0.7.5        # via ipython
pillow==8.2.0             # via cairosvg
ply==3.11                 # via plyara
plyara==2.0.3
prompt-toolkit==2.0.10    # via click-repl, ipython
psutil==5.6.7
psycopg2-binary==2.8.5
ptyprocess==0.6.0         # via pexpect
punq==0.4.1
pyasn1==0.4.8             # via paramiko
pycparser==2.20           # via cffi
pygments==2.7.4           # via ipython, pdbpp
pyjwt==1.7.1
pyldap==2.4.25.1
pymisp==2.4.121
pynacl==1.4.0             # via paramiko
pyopenssl==19.1.0         # via pysaml2
pyotp==2.3.0
pyphen==0.9.5             # via weasyprint
pyrepl==0.9.0             # via fancycompleter
pyrsistent==0.16.0        # via jsonschema
pysaml2==6.5.1
python-dateutil==2.8.0
python-editor==1.0.4      # via alembic
```

```
python-gnupg==0.4.4
python-magic==0.4.15
python-slugify==3.0.3
pytz==2017.3
pyyaml==5.4
quuz==9.0.0
rarfile==3.0.0
redis==3.5.3
regex==2020.6.8           # via dateparser
requests-futures==0.9.9
requests==2.25.1
retrying==1.3.3
rfc3986==1.2.0
s3transfer==0.1.13        # via boto3
sanest==0.1.0
simplejson==3.17.0        # via stix2
six==1.15.0               # via bcrypt, cabby, click-repl, elasticsearch-curator, furl,
html5lib, jsonlines, jsonschema, libtaxii, opentaxii, orderedmultidict, prompt-toolkit,
pymisp, pynacl, pyopenssl, pyrsistent, pysaml2, python-dateutil, retrying, stix2, stix2-
patterns, structlog, taxii2-client, tld, traitlets, validators
sos==3.5.1-eiq
soupsieve==2.0.1          # via beautifulsoup4
sqlalchemy==1.3.22
statsd==3.3.0
stix-validator==2.5.0
stix2-patterns==1.3.2
stix2[taxii]==2.1.0
structlog==20.1.0
tabulate==0.8.5
taxii2-client==2.2.2
text-unidecode==1.2       # via python-slugify
tinycss2==1.0.2           # via cairosvg, cssselect2, weasyprint
tld==0.7.9
traitlets==4.3.3          # via ipython
typing-extensions==3.7.4.3  # via quuz
tzlocal==2.1              # via dateparser
uritools==3.0.0           # via urlextract
urlextract==0.13.0
urllib3==1.25.9           # via elasticsearch, elasticsearch-curator, requests
validators==0.15.0
vine==5.0.0               # via amqp, celery
voluptuous==0.12.0        # via elasticsearch-curator
wcwidth==0.2.4            # via prompt-toolkit
weasyprint==51
webencodings==0.5.1       # via cssselect2, html5lib, tinycss2
werkzeug==1.0.1
wheel==0.33.6
wmctrl==0.3               # via pdbpp
xlrd==1.2.0               # via stix-validator
xmlschema==1.5.3          # via pysaml2
xmltodict==0.11.0
zipp==3.1.0               # via importlib-metadata, importlib-resources
zxcvbn==4.4.27

# The following packages are considered to be unsafe in a requirements file:
pip==19.1.1
setuptools==45.1.0
```

Frontend dependencies

```
"@draft-js-plugins/alignment": "^4.1.0",
"@draft-js-plugins/drag-n-drop": "^4.1.0",
"@draft-js-plugins/editor": "^4.1.0",
"@draft-js-plugins/focus": "^4.1.0",
"@draft-js-plugins/image": "^4.1.0",
"@draft-js-plugins/resizeable": "^4.1.0",
"@headlessui/react": "^0.2.0",
"@popperjs/core": "^2.9.2",
"@sentry/browser": "^5.12.1",
"@types/draft-js": "^0.10.44",
"autoprefixer": "^10.0.4",
"classnames": "^2.2.6",
"clipboard-copy": "^3.1.0",
"debug": "^2.6.3",
"dompurify": "2.2.2",
"draft-convert": "^2.1.4",
"draft-js": "^0.11.7",
"enzyme-adapter-react-16": "^1.0.1",
"escape-string-regexp": "^1.0.5",
"filesize": "^3.5.6",
"flux": "^2.0.1",
"he": "^1.1.1",
"history": "^4.6.1",
"image-size": "^0.5.0",
"immutability-helper": "^2.4.0",
"immutable": "^3.7.4",
"json-stable-stringify": "^1.0.1",
"jwt-decode": "^2.2.0",
"keycode": "^2.2.0",
"keylines": "file:./src/vendor/keylines",
"keymirror": "~0.1.0",
"lint-staged": "^10.5.4",
"lodash": "^4.17.21",
"markdown-it": "^10.0.0",
"markdown-it-regexp": "^0.4.0",
"microdata": "^1.1.3",
"moment": "2.24.0",
"moment-timezone": "0.5.3",
"patch-package": "^6.2.2",
"pluralize": "^8.0.0",
"postinstall-postinstall": "^2.1.0",
"qrcode": "^1.4.4",
"qs": "^6.0.2",
"raw-loader": "^0.5.1",
"react": "^16.11.0",
"react-addons-shallow-compare": "^15.6.2",
"react-click-outside": "^2.1.0",
"react-dates": "17.0.0",
"react-dnd": "^11.1.3",
"react-dnd-html5-backend": "^11.1.3",
"react-dom": "^16.11.0",
"react-dropzone": "^3.3.2",
```

```
    "react-filtered-multiselect": "^0.4.2",
    "react-immutable-proptypes": "^1.5.0",
    "react-mixin": "^3.0.3",
    "react-pdf": "^4.0.0",
    "react-popper": "^2.2.5",
    "react-redux": "^5.0.7",
    "react-resize-detector": "^5.2.0",
    "react-router": "^5.2.0",
    "react-router-dom": "^5.2.0",
    "react-select": "1.0.1",
    "react-split": "^2.0.9",
    "react-string-replace": "^0.3.2",
    "react-tether": "^1.0.4",
    "react-time-picker": "^1.1.0",
    "react-treeview": "^0.4.2",
    "react-use": "^17.2.3",
    "redux": "^4.0.0",
    "redux-devtools-extension": "^2.13.8",
    "reselect": "^3.0.1",
    "scrollbar-width": "^3.1.1",
    "superagent": "^3.8.1",
    "superagent-promise": "^1.1.0",
    "superagent-throttle": "1.0.0",
    "tailwindcss-classnames": "^2.0.7",
    "tailwindcss-interaction-variants": "^5.0.0",
    "tcomb-form": "0.9.20",
    "transit-immutable-js": "^0.5.2",
    "transit-js": "^0.8.846",
    "typed-immutable": "0.0.7",
    "word-wrap": "^1.2.3"
  },
```

Functionality

This section describes EclecticIQ Platform key features and functionality such as authentication and authorization, ingestion and dissemination, as well its user-facing and programmatic interfaces.

Authentication and authorization

User management

EclecticIQ Platform enables managing application users, user groups, roles, as well as viewing permissions.

Upon user creation, newly created users receive a notification email with a link to update their profile and set their password.

Admin users can create, edit, and disable platform users.

User access to the platform relies on an authentication and authorization mechanism.

User access to threat intelligence data in the platform is controlled based on:

- The groups to users belong to.
- The allowed data sources user groups are granted access to.
- The TLP code platform entities are flagged with.

It is possible to set password complexity and to define lockout policies to match organizational needs and requirements.

When choosing a password policy, we recommend following NIST Digital Identity Guidelines[15].

User authentication and authorization

The platform authenticates users based on its internal users.

You can manage authentication, authorization, and access rights for groups and roles, as well as user membership to one or more groups.

EclecticIQ Platform manages and controls resource access and consumption by defining access profiles at different access tiers with the following characteristics:

- **Users:** individual platform consumers.
  They can access the platform by signing in with their designated account credentials, such as user name and password.
  Example: *mhamilton / Apollo11*
- **Groups:** multiple users brought together under a common umbrella.
  They share the same access rights to selected allowed data sources, such as specific datasets, feeds, enrichers, as well as other groups.
  Example: *Threat analysts*
  User groups enable controlling user group members' access to specific platform data, assets, and resources through the following mechanisms:
  - **Allowed sources:** data origins of content stored in the platform.
    Selecting an allowed data source for a group means that all group members can access platform content that the data source in question is the producer of.

15 https://pages.nist.gov/800-63-3/sp800-63b.html

Data sources can be existing incoming feeds, enrichers, as well as other user groups.
Example: *Entities from Feed A*

- **TLP:** TLP stands for Traffic Light Protocol[16].
  TLP color codes flag information to provide handling and sharing guidelines.
  You can assign a TLP color value to restrict access to the following platform items:
  - Entities.
  - Data you receive via incoming and send out via outgoing feeds.
  - Data created by users belonging to the groups associated with allowed data sources.

- **Roles:** the expected functions assigned to an individual user or to a group of users.
  Roles represent sets of actions users can be tasked with.
  Roles group sets of permissions to define the allowed read and modify behaviors that are appropriate to the functions they are related to.
  Example: *Team lead*
- **Permissions:** rules and policies constraining user scope.
  Permissions delimit scope by defining the types of action users are authorized to carry out.
  For example: *read; modify* (that is, create, edit, and delete.)

- Role-based permissions define:
  - The type of actions users are allowed to perform.
  - The type of objects users are allowed to interact with.
- Group-based **Allowed sources** and **TLP** define:
  - Specific platform data, assets, and resources users are allowed to access.

External authentication

Alternatively, it can retrieve the necessary information from an external LDAP server.

LDAP integration enables importing existing users from an LDAP server.

Upon successful authentication, users are issued a JSON web token (JWT) that grants them access.

16 https://www.us-cert.gov/tlp

JWTs expire automatically; when this happens, the platform automatically issues a new JWT.

All REST services exposed through the platform accept and validate JWT, so that the application is truly stateless.

EclecticIQ Platform supports also SAML v2 authentication via SSO.

The integration requires at least the following properties:

- Userid
- Email
- Groups
- Roles

Permissions

The following are the most granular permissions available in EclecticIQ Platform:

Permission	Purpose	Behavior in the platform
install configuration-bundles	Allows user to install /get-to-know-the-platform/knowledge-packs. Users must also have `read configuration-bundles` permissions to be able to install knowledge packs.	With the permission • Can install knowledge packs.
lock/unlock users	Enables unlocking users whose account has been locked[17] after too many failed login attempts.	With the permission: • Users with a locked account can request request unlocking[18] it. Without the permission: • **Unlock** is not available to users whose account status is **Locked**.

17 https://docs.eclecticiq.com/get-to-know-the-platform/users/manage-users#Manageusers-lock-users
18 https://docs.eclecticiq.com/get-to-know-the-platform/users/manage-users#Manageusers-unlock-users

Permission	Purpose	Behavior in the platform
modify blob-uploads	Enables manually uploading files[19] for ingestion into the platform through the **Upload** option and the **Uploads** tab.	With the permission: • The **Uploads** tab is visible to users, and they can access it. • Users can manually upload files to the platform. Without the permission: • The **Uploads** tab is not available. • Users cannot manually upload files to the platform.
modify collaborators	Enables workspace owners and collaborators to add and to remove users to and from workspaces they belong to.	With the permission: • Workspace owners/creators can click ⊕ in the top-right corner of the workspace view to add other users as collaborators to the active workspace. • Workspace collaborators can click ⊕ in the top-right corner of the workspace view to add other users as collaborators to the active workspace. Without the permission: • The ⊕ option to add users to the workspace is not available. • Users cannot add other users as collaborators to a workspace.

19 https://docs.eclecticiq.com/work-with-intelligence/entities/manage-entities/manually-upload-files

Permission	Purpose	Behavior in the platform
modify configurations	Enables viewing and editing system configuration options[20] in the **System settings** view and its tabs, as well as the **STIX** and **TAXII** settings available in the **STIX** and **TAXII** view.	With the permission: • Users can access and view system configuration options available in the following **System settings** tabs: ◦ **General** ◦ **Proxy** ◦ **Email** ◦ **License** ◦ **Intel report** ◦ **Private key** ◦ **Trusted keys** ◦ **System** ◦ **Account policy** ◦ They cannot edit settings in the **Audit** tab. • Users can access and edit system configuration options available in the following **STIX and TAXII** tabs: ◦ STIX ◦ TAXII Without the permission: • Users cannot access any system settings configuration options.
modify configuration-bundles	Allows user to modify knowledge packs.	Not available for 2.10 and earlier.

20 https://docs.eclecticiq.com/install-configure-upgrade/configure-the-platform-settings

Permission	Purpose	Behavior in the platform
modify discovery-rules	Enables viewing and editing discovery rules[21].	With the permission: • Users can create and modify discovery rules. Users can access the menu options available by clicking ⋮, and they can carry out the following actions on discovery rules: • Run[22] the selected rule. • Enable and disable[23] the selected rule. • Edit[24] and delete[25] the selected rule. Without the permission: • Users cannot create or modify discovery rules. • The options available by clicking are not available.

21 https://docs.eclecticiq.com/get-to-know-the-platform/rules/discovery-rules
22 https://docs.eclecticiq.com/get-to-know-the-platform/rules/discovery-rules/manually-run-discovery-rules
23 https://docs.eclecticiq.com/get-to-know-the-platform/rules/discovery-rules/enable-and-disable-discovery-rules
24 https://docs.eclecticiq.com/get-to-know-the-platform/rules/discovery-rules/edit-discovery-rules
25 https://docs.eclecticiq.com/get-to-know-the-platform/rules/discovery-rules/delete-discovery-rules

Permission	Purpose	Behavior in the platform
modify draft-entities	Enables viewing and editing draft entities[26].	With the permission: • Users can create and modify draft entities. • In the entity editor, users can click **Save draft** to save a manually created entity as a draft for further refining at a later time. Without the permission: • Users cannot access the entity editor, unless they have the **modify entities** permission. • In the entity editor, the **Save draft** option is not available, and users cannot save a manually created entity as a draft. ⓘ To access the entity editor, users need at least one of the following permissions: • **modify draft-entities** • **modify entities**
modify enrichers	Enables viewing and editing enrichers[27], as well as enabling and disabling them[28].	With the permission: • Users can enable and disable enrichers. • Users can edit enricher configuration settings in the **Edit enricher task** view. Without the permission: • Users cannot enable or disable enrichers. • The **Edit** option to modify enricher configuration settings is not available.

26 https://docs.eclecticiq.com/work-with-intelligence/entities/create-entities/draft-and-published-entities
27 https://docs.eclecticiq.com/integrations/extensions/enrichers/configure-enrichers
28 https://docs.eclecticiq.com/integrations/extensions/enrichers/enable-and-disable-enrichers

Permission	Purpose	Behavior in the platform

modify enrichment-rules	Enables viewing, creating, and editing enrichment rules.	With the permission:
		• Users can create and modify enrichment rules.
		• Users can access the menu options available by clicking ⋮, and they can carry out the following actions on enrichment rules:
		  ◦ Enable and disable the selected rule.
		  ◦ Edit and delete the selected rule.
		Without the permission:
		• Users cannot create or modify enrichment rules.
		• The options available by clicking ⋮ are not available.

modify enrichments	Enables editing manual enrichment objects[29]. They are enrichment observables resulting from a manual enrichment action on an entity or an observable.	This permission is not implemented for use through the platform GUI.

29 https://docs.eclecticiq.com/get-to-know-the-platform/rules/enrichment-rules/enrich

Permission	Purpose	Behavior in the platform
modify entities	Enables viewing, creating, editing, and deleting entities[30].	With the permission: • Users can create and modify entities. • In the entity editor, users can click **Publish** to save and publish a manually created entity. Without the permission: • Users cannot access the entity editor, unless they have the **modify draft-entities** permission. • In the entity editor, the **Publish** option is not available, and users cannot save and publish a manually created entity. ⓘ To access the entity editor, users need at least one of the following permissions: • **modify draft-entities** • **modify entities**

30 https://docs.eclecticiq.com/work-with-intelligence/entities

Permission	Purpose	Behavior in the platform
modify extracts	Enables creating and editing observables[31].	With the permission: • Users can create and modify observables. • Users can access the Add observable view through the **Observables** tab, the **+ Create observable**, the **+ Add observable**, or the **+ Observable** options. Without the permission: • Users cannot create or modify observables. • Users cannot access the **Add observable** view.
modify files	Enables manually attaching files to a workspace, pinning them to a workspace front page, modifying files belonging to a workspace, and removing them from a workspace.	With the permission: • Workspace owners and collaborators can attach, pin, and delete files to and from the workspaces the belong to, as well as edit workspace files. Without the permission: • Attempts to attach, pin, edit, or delete files to or from a workspace are either not available, or they are grayed out in the GUI.
modify graphs	Enables editing graphs[32].	With the permission: • Users can load objects to a graph; they can create, edit, and save graphs. Without the permission: • Users cannot modify existing graphs or create new ones.

31 https://docs.eclecticiq.com/work-with-intelligence/observables
32 https://docs.eclecticiq.com/get-to-know-the-platform/graphs/add-entities-to-a-graph

Permission	Purpose	Behavior in the platform
modify groups	Enables viewing, creating, editing, and deleting user groups[33]. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read users**	With the permission: • Users can create, save, modify, and delete user groups. • For example, they can modify a user group to: ◦ Add and remove users. ◦ Add and remove **Allowed sources**. ◦ Change the **TLP** color code associated with an allowed source to modify the group access rights to the corresponding data source. ◦ Change the default **Source reliability** value assigned to a group. ◦ Group administrators can add and remove roles to modify the user access options available for the group. Without the permission: • Users cannot create, save, modify, or delete user groups. • The **+ Create group** option is not available.

33 https://docs.eclecticiq.com/get-to-know-the-platform/users/manage-groups

Permission	Purpose	Behavior in the platform
modify incoming-feeds	Enables viewing, creating, editing, and deleting incoming feeds[34].	With the permission: • Users can create, save, edit, delete, and purge incoming feeds. Without the permission: • Users cannot create, save, edit, delete, or purge incoming feeds. • Attempts to edit the selected feed, to retry downloading, or to ignore failed packages are either not available, or they are grayed out in the GUI.
modify intel-sets	Enables viewing, creating, editing, and deleting datasets[35].	With the permission: • Users can create, save, edit, and delete datasets. • Users can add search result items to datasets. Without the permission: • Users cannot create, save, edit, or delete datasets. • Users cannot add search result items to datasets. • Attempts to edit or to delete datasets from the dataset overview list and the dataset detail pane are either not available, or they are grayed out in the GUI.
modify kibana	Enables viewing, creating, editing, and deleting native Kibana dashboards.	This permission is not implemented for use through the platform GUI. Users can access it through the Kibana GUI[36].

34 https://docs.eclecticiq.com/integrations/extensions/incoming-feeds
35 https://docs.eclecticiq.com/get-to-know-the-platform/datasets
36 https://docs.eclecticiq.com/get-to-know-the-platform/search/search-query-fields

Permission	Purpose	Behavior in the platform
modify outgoing-feeds	Enables viewing, creating, editing, and deleting outgoing feeds[37].	With the permission: • Users can create, save, edit, delete, and purge outgoing feeds. Without the permission: • Users cannot create, save, edit, delete, or purge outgoing feeds. • Attempts to edit or to delete outgoing feeds from the outgoing feed overview list and the outgoing feed detail pane are either not unavailable, or they are grayed out in the GUI. • Users can access the GUI options to delete or to disable outgoing feeds from the outgoing feed overview list and the outgoing feed detail pane. • However, clicking these options returns an error. • A deleted outgoing feed is temporarily removed from the outgoing feed list, but it is added again to the list after refreshing the view.

37 https://docs.eclecticiq.com/integrations/extensions/outgoing-feeds

Permission	Purpose	Behavior in the platform
modify retention-policies	Enables viewing, creating, editing, enabling, running, disabling, and deleting .	With the permission: • Users can create, save, edit, and delete . • Users can enable and disable[38] data retention policies. • User can run data retention policies[39], either manually, or based on a predefined schedule. Without the permission: • Users cannot perform any actions to modify or to run data retention policies. • If they have the **read retention-policies** permission, they can access the data retention policies overview, where they can select policies to review them in read-only mode by clicking **Data configuration > Policies** in the top navigation bar. • If they do not have the **read retention-policies** permission, the corresponding GUI options are not available.
modify roles	Enables viewing, creating, editing, and deleting roles. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read users**	With the permission: • Users can create, save, edit, and delete roles. • Users can add an remove permissions to and from roles. Without the permission: • Users cannot create, save, edit, and delete roles. • The corresponding GUI options are not available.

38 https://docs.eclecticiq.com/get-to-know-the-platform/policies/data-policies/enable-and-disable-data-policies
39 https://docs.eclecticiq.com/get-to-know-the-platform/policies/data-policies/run-data-policies

Permission	Purpose	Behavior in the platform
modify rules	Enables viewing, creating, editing, and deleting entity[40] and observable[41] rules.	With the permission: • Users can create modify entity and observable rules. • Users can access the menu options available by clicking ⋮, and they can carry out the following actions on entity and observable rules: ◦ Run the selected rule. ◦ Enable and disable the selected rule. ◦ Edit and delete the selected rule. Without the permission: • Users cannot create or modify entity or observable rules. • The options available by clicking ⋮ are not available.

40 https://docs.eclecticiq.com/get-to-know-the-platform/rules/entity-rules
41 https://docs.eclecticiq.com/get-to-know-the-platform/rules/observable-rules

Permission	Purpose	Behavior in the platform
modify tasks	Enables viewing and editing enrichment tasks[42], as well as stopping currently running system jobs.	With the permission: • Users can modify enrichment tasks defining enricher behavior. • Users can access the **Edit enricher task** view by clicking an enricher tile in the enricher overview, and then by clicking **Edit** on the enricher detail pane. • Users can terminate currently running system jobs. • Users can access the **Terminate** option on the job detail pane by selecting a running job in the **System jobs**, **Running** view. Without the permission: • Users cannot modify enrichment tasks. • The **Edit** on the enricher detail pane and the **Edit enricher task** view are not available. • Users cannot terminate currently running system jobs. • On the job detail pane, the **Terminate** option is not available.

42 https://docs.eclecticiq.com/integrations/extensions/enrichers/edit-enricher-tasks

Permission	Purpose	Behavior in the platform
modify taxii-services	Enables viewing and editing global STIX and TAXII configuration options.	With the permission: • Users can modify global STIX and TAXII configuration settings for the platform. • Users can access the STIX and TAXII options by clicking ⚙, and then **System settings** in the left navigation bar. Without this permission: • Users cannot modify global STIX and TAXII configuration settings. • The **STIX** and **TAXII** views are not available through ⚙ in the left navigation bar.

Permission	Purpose	Behavior in the platform
modify taxonomies	Enables viewing, creating, editing, and deleting taxonomies[43].	With the permission: • Users can create new taxonomies, and they can populate them with parent and child tags. • Users can access the options to create, edit, and delete taxonomies and by clicking **Data configuration > Taxonomies** in the top navigation bar. Without this permission: • Users cannot create new taxonomies, and they cannot modify or delete existing ones. • If they have the **read taxonomies** permission, they can: ◦ Access The **Taxonomies** view by clicking **Data configuration > Taxonomies** in the top navigation bar. ◦ View taxonomy and tag details in entity and observable detail panes.

43 https://docs.eclecticiq.com

Permission	Purpose	Behavior in the platform
modify ticket-comments	Enables viewing, creating, and editing comments to user tasks[44] in workspaces, and in the **Tasks** view. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **modify tickets**	With the permission: • Users can add comments to existing user tasks[45] in workspaces, as well as edit and delete them. • Users can add comments to user tasks in the following platform areas: ◦ Workspaces[46] ◦ Tasks[47] • In the task detail pane, they can access the ✎ and 🗑 options to edit and delete an existing comment, respectively. Without the permission: • Users can access user task comments in read-only mode. • In the user task detail pane, the ✎ and 🗑 options are not available.

44 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces/collaborate-with-other-users/create-user-tasks
45 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces/collaborate-with-other-users/write-and-review-comments
46 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces
47 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces/collaborate-with-other-users/view-tasks

Permission	Purpose	Behavior in the platform
modify tickets	Enables viewing, creating, and editing user tasks[48] in workspaces, and in the **Tasks** view. ⓘ The following permissions require **modify tickets** as a dependency to work as expected: • **modify ticket-comments**	With the permission: • Users can create user tasks, assign and reassign them to user task owners and stakeholders, set deadlines and progress statuses, close and reopen them, and so on. • Users can create user tasks in the following platform areas: ◦ Workspaces ◦ Tasks • Users can access the GUI options to create, modify, and delete user tasks in the **Tasks** view, as well as the menu options available by clicking ⋮ in the **Tasks** view to edit, reassign, change the deadline, close and reopen the task, as well as cancel and delete it. Without the permission: • Users cannot create or modify user tasks in workspaces. • The corresponding GUI options in the **Tasks** view, as well as the menu options available by clicking ⋮ in the **Tasks** view, are not available.

48 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces/collaborate-with-other-users/create-user-tasks

Permission	Purpose	Behavior in the platform
modify users	Enables viewing, creating, editing, and deactivating users. Extensible: • **modify user-groups** adds the ability to assign and to remove users to and from groups. • **modify user-roles** adds the ability to assign and to remove roles to and from users.	With the permission: • Users can create, edit, and deactivate platform user profiles[49]. • Users can access the relevant GUI options to carry out these actions. • Users can change users' personal details. • In combination with the **modify user-groups** permission: users can also assign users to groups, and remove them. • In combination with the **modify user-roles** permission: users can also assign roles to users, and remove them. Without the permission: • Users cannot create, edit, or deactivate platform user profiles. • The GUI options to create and edit user profiles are not available.

49 https://docs.eclecticiq.com/get-to-know-the-platform/users/manage-users

Permission	Purpose	Behavior in the platform
modify user-groups	Enables adding and removing users to and from user groups. This permission can extend: • **modify users**	With the permission: • Users can edit user profiles by adding users to and removing them from groups. • Users can edit user profiles by assigning user types for the selected groups: ◦ **Group admin** ◦ **Member** • Users can access the GUI options to add users to and remove them from groups. Without the permission: • Users cannot add users to or remove them from groups, and they cannot assign user types. • The corresponding GUI options are not available. • Users can edit their own user profile.

Permission	Purpose	Behavior in the platform
modify user-roles	Enables assigning and removing roles to and from users to extend or to limit user access scope. This permission can extend: • **modify users**	With the permission: • Users can assign and remove roles to and from users to extend or to limit the access scope of a user. • Users can access the GUI options in the edit user view to assign and to remove roles to and from user profiles. Without the permission: • Users cannot modify users by adding or removing roles. • Users can access the corresponding GUI options in the edit user view. However, they cannot save any changes they may attempt to make to the currently assigned roles for the user. If they have the **read users** and the **read roles** permissions, they can: • View any roles assigned to a user in the user detail pane.

Permission	Purpose	Behavior in the platform
modify workspace-comments	Enables viewing, creating, editing, and deleting workspace comments[50]. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **modify workspaces**	With the permission: • In a workspace **Comments** view, workspace collaborators can create workspace comments by typing text in the input field, and then by pressing **ENTER**. • In a workspace **Comments** view, workspace collaborators can access the ✎ and 🗑 options to edit and delete an existing comment, respectively. Without the permission: • Workspace collaborators can view existing comments with read-only access. • Workspace collaborators cannot create workspace comments, and they cannot edit or delete existing workspace comments.
modify workspaces	Enables viewing, creating, editing, and deleting workspaces[51]. ⓘ The following permissions require **modify workspaces** as a dependency to work as expected: • **modify workspace-comments**	With the permission: • Workspace collaborators can create, edit, archive, and delete workspaces. • Workspace collaborators can access the relevant GUI options to carry out these actions. Without the permission: • User have access to the GUI options to create and to edit workspaces. • Any actions attempting to save a new workspace, or to edit an existing one are either completely unavailable, or they are grayed out in the GUI.

50 https://docs.eclecticiq.com
51 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces

Permission	Purpose	Behavior in the platform
read audit-trail	Enables viewing the audit trail in the **Audit** view under **System settings**. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read configurations**	With the permission: • Users can access and view the audit trail by clicking ⚙, **System settings**, and **Audit**. • Users can sort events by column header. • Users can enter search queries in the search input field to look for events, and they can filter events with quick filter options. Without the permission: • Users cannot access the audit trail. • The **Audit** option and the corresponding view are not available.
read attack	Allows access to the MITRE ATT&CK built-in taxonomy on the platform. Users must have this permission and `modify entities` to be able to assign ATT&CK classifications to an entity. For more information, see /work-with-intelligence/mitre-attack	With the permission: • View list of ATT&CK classifications in **Create ATT&CK classification** modal. Without the permission • Can still search entities by ATT&CK classifications. • Can still view ATT&CK classifications assigned to entities. • Cannot assign ATT&CK classifications to entities.

Permission	Purpose	Behavior in the platform
read blob-uploads	Enables viewing a list with recently uploaded files.	With the permission: • In the **Uploads** tab under **Browse**, users can see a list of recently uploaded files under the **Recently uploaded files** header. Without the permission: • Users can access the **Uploads** tab under **Browse**. However, they cannot view any manually uploaded content under **Recently uploaded files**.
read collaborators	Enables viewing workspace collaborators.	With the permission: • Workspace owners and collaborators can see collaborators of the workspaces they belong to. Without the permission: • It is not possible to see collaborators of the workspaces users belong to.

Permission	Purpose	Behavior in the platform
read configurations	Enables viewing system configuration options in the **System settings** view and its tabs, as well as the **STIX** and **TAXII** settings available in the **STIX** and **TAXII** view.	With the permission: • Users can access and view system configuration options available in the following **System settings** tabs: ◦ **General** ◦ **Proxy** ◦ **Email** ◦ **License** ◦ **Intel report** ◦ **Private key** ◦ **Trusted keys** ◦ **System** ◦ **Account policy** ◦ They cannot edit settings in the **Audit** tab. • Users can access and edit system configuration options available in the following **STIX and TAXII** tabs: ◦ STIX ◦ TAXII Without the permission: • Users cannot access, and they cannot view any system settings configuration options.
read configuration-bundles	Allows users to view knowledge packs.	With this permission: • Can view knowledge packs.

Permission	Purpose	Behavior in the platform
read content-blocks	Enables viewing outgoing feed package overviews in outgoing feed detail panes.	With the permission: • The **Created packages** in outgoing feed detail panes displays a list of content packages created after completing a successful outgoing feed task run. Without the permission: • The **Created packages** in outgoing feed detail panes does not display any package content. Users receive an error message.
read content-types	Enables viewing outgoing feed content type information, including the content type drop-down menu options in the feed editor.	With the permission: • Users can view the content type of an outgoing feed. • In the feed editor, users can access the **Content type** drop-down menu to select a content type for an outgoing feed. Without the permission: • Users cannot view the content type of an outgoing feed. • In the feed editor, the **Content type** drop-down menu options are not available.

Permission	Purpose	Behavior in the platform
read destinations	Enables viewing the destinations of entities or observables published through outgoing feeds.	With the permission: • In the **Overview** tab of entity and observable detail panes users can view a list of outgoing feeds used to disseminate the entity or observable. The list is available under the **Destinations** header. Without the permission: • In the **Overview** tab of entity and observable detail panes users cannot view the outgoing feeds used to disseminate the entity or observable.
read discovery-rules	Enables viewing discovery rules.	With the permission: • Users can access and view discovery rules in the **Discovery** tab under **Rules**. • Users can enable and disable on-screen notifications about discovered entities matching the active discovery rules. Without the permission: • Users cannot access or view discovery rules. • Users on-screen notifications about discovered entities matching the active discovery rules are not available.

Permission	Purpose	Behavior in the platform
read draft-entities	Enables viewing draft entities tab in the **Draft** tab under **Production**.	With the permission: • View draft entities. • **Create + > VIEW PRODUCTION > Drafts** is available. Without the permission: • Users cannot access draft entities. • The **Draft** tab is not available.
read enrichers	Enables viewing available enrichers in the **Enrichers** view and by sending a request to the enricher API endpoint.	With the permission: • Users can view available platform enrichers by clicking **Data configuration**, **Enrichers**. • Users can send a request to the `/api/enrichers/` endpoint to retrieve a list of available platform enrichers, along with their current configuration settings. • Users can view enricher status: either enabled or disabled. Without the permission: • The **Enrichers** view is not available. • It is not possible to make successful requests to the `/api/enrichers/` endpoint. • Enricher status is not available.

Permission	Purpose	Behavior in the platform
read enrichment-rules	Enables viewing enrichment rules[52], along with rule details and configuration.	With the permission: • Users can view available enrichment rules by clicking **Data configuration**, **Rules**, **Enrichment**. • Users can view enrichment rule status: either enabled or disabled. Without the permission: • The **Enrichment** tab is not available. • Attempts to directly access the **Enrichment** tab by copy-pasting the corresponding URL into the browser address bar return a 403 Forbidden HTTP status code. • Enrichment rule status is not available.
read enrichments	Enables viewing manual enrichment results.	This permission is not implemented for use through the platform GUI.

52 https://docs.eclecticiq.com/get-to-know-the-platform/rules/enrichment-rules

Permission	Purpose	Behavior in the platform
read entities	Enables viewing entities.	With the permission: • Users can access and view entities inside workspaces, and in the following views: ◦ **Browse** ◦ **Production** ◦ **Discovery** ◦ **Exposure** • Users can search for entities. Without the permission: • Users cannot access or view entities anywhere in the platform. • Entity searches return a permission error. • The following views are not available: ◦ **Browse** ◦ **Production** ◦ **Discovery** • In the **Exposure** view, **Entities** tab, a permissions error is displayed. • Workspace content is not available.

Permission	Purpose	Behavior in the platform
read extracts	Enables viewing observable objects and observable data in the platform main dashboard.	With the permission: • Users can access and view observables inside workspaces, and in the following views: ◦ **Browse** ◦ **Production** ◦ **Discovery** ◦ **Exposure** • Users can search for observables. Without the permission: • Users can view the platform main dashboard. However, the dashboard does not include observable data. • Observable searches return a permission error. • Users can open and view observable detail panes. However, the detail pane displays a permission error. • Users can view a list of observables related to an entity in the entity detail pane, as well as existing observables in the **Browse** and **Production** views. However, it is not possible to access observable information by clicking an observable to display the corresponding detail pane.

Permission	Purpose	Behavior in the platform
read files	Enables viewing manually uploaded files.	With the permission: • Users can view and download manually uploaded files in the **Uploads** tab under **Browse**. • Users can view and download manually uploaded files belonging to a dataset in a workspace. Without the permission: • Users cannot view or download any manually uploaded files.
read graphs	Enables accessing and viewing the graph.	With the permission: • is available in the left navigation menu. • Users can load objects to display them on the graph. • They can export populated graphs to png format only. Without the permission: • is not available in the left navigation menu. • The **Add to graph** menu option is disabled. • Workspace overview tiles show a counter indicating how many saved graphs a workspace contains. However, it is not possible to view saved graphs inside workspaces.

Permission	Purpose	Behavior in the platform
read groups	Enables viewing user groups. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read users**	With the permission: • Users can view existing groups by clicking ⚙, **User management > Groups**, **Groups**. • In the user detail pane it is possible to see which groups a user belongs to. Without the permission: • Users cannot view user groups. • The **Groups** view is not available. • In the user detail pane no user group details are available.
read history-events	Enables viewing historical information related to events and actions applied to platform objects.	With the permission: • Users can access the **History** tab on the detail panes of users, groups, roles, incoming and outgoing feeds, rules, policies, graphs, workspaces, and entities. • Users can view historical information related to users, groups, roles, incoming and outgoing feeds, rules, policies, graphs, workspaces, and entities. Without the permission: • The **History** tab is not available on any detail panes. • Historical information is not available.

Permission	Purpose	Behavior in the platform
read incoming-feeds	Enables viewing incoming feeds.	With the permission: • Users can access and view incoming feeds by clicking **Data configuration**, **Incoming feeds**. • Users can click incoming feed names to open the corresponding detail panes, and to view more information about the selected incoming feed. Without the permission: • The **Incoming feeds** view is not available. • Incoming feed detail panes are not available.
read intel-sets	Enables viewing datasets.	With the permission: • Users can access and view datasets in **Search** ? Unknown Attachment **> GO TO SEARCH AND BROWSE > Datasets**. Without the permission: • The **Datasets** view is not available. • Dataset detail panes are not available.

Permission	Purpose	Behavior in the platform

read notifications	Enables viewing platform notifications and the corresponding menu.	With the permission:
		• In the left navigation bar 🔔 is available.
		• By clicking it, users display a notification pop-up pane with the following notification display tabs:
		  ◦ Updates
		  ◦ Actions
		• Users can access and view update notifications about platform events – for example, the creation of a new feed or the discovery of new entities – as well as notifications about user actions – for example. reloading a working draft.
		• Users can select the events they wish to be notified about.
		Without the permission:
		• In the left navigation bar 🔔 is not available.
		• The notification pop-up pane with the **Updates** and the **Actions** notification display tabs is not available.

Permission	Purpose	Behavior in the platform
read outgoing-feeds	Enables viewing outgoing feeds.	With the permission: • Users can access and view outgoing feeds by clicking **Data configuration**, **Outgoing feeds**. • Users can click outgoing feed names to open the corresponding detail panes, and to view more information about the selected outgoing feed. Without the permission: • The **Outgoing feeds** view is not available. • Outgoing feed detail panes are not available. • Attempts to directly access an outgoing feed by copy-pasting the corresponding URL into the browser address bar return a **401 Unauthorized** HTTP status code. • In dataset detail panes the **Outgoing feeds** section is not available. • When users delete a dataset from a workspace, they receive a pop-up dialog listing any workspaces, outgoing feeds, and entity rules associated with the dataset. Outgoing feeds are not available in this overview for users without the permission.

Permission	Purpose	Behavior in the platform
read permissions	Enables viewing the list of available permissions for the platform. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read users**	With the permission: • Users can access and view the permission overview listing the available permissions for the platform by clicking ⚙, **User management**, **Permissions**. Without the permission: • The **Permissions** view is not available.
read retention-policies	Enables viewing .	With the permission: • Users can view . • Users can access the data retention policies overview, where they can select policies to review them in read-only mode by clicking • In the top navigation bar click **Data configuration > Policies**. Without the permission: • Users cannot access data retention policies. • The In the top navigation bar click **Data configuration > Policies** view is not available in the GUI.

Permission	Purpose	Behavior in the platform
read roles	Enables viewing the overview of available roles in the platform, as well as the roles assigned to a user in the user profile edit view. EclecticIQ Platform ships with the following predefined roles: • **Threat Analyst**: this role can read and manage workspaces and threat intelligence data. This role cannot manage users and system services. • **Team Lead**: besides having the same permission set as the Threat Analyst role, this role can assign users to groups, as well as modify user group membership. • **System Admin**: this role can manage incoming and outgoing feeds, enrichers, users, groups, and other system settings. This role has limited access to workspaces and threat intelligence data. ⓘ To work as expected, this permission requires the following permissions as dependencies: ◦ **read users**	With the permission: • Users can access and view the role overview listing the available roles for the platform by clicking ⚙, **User management**, **Roles**. • Users can view any assigned user roles in the user detail pane. Without the permission: • The **Roles** view is not available.

Permission	Purpose	Behavior in the platform
read rules	Enables viewing the list of available entity and observable rules for the platform.	With the permission: • Users can access and view lists of existing observable and entity rules by clicking **Data configuration**, **Rules**. • The **Observable** and the **Entity** tabs with the existing observable and entity rules are available. • Users can click a rule to display the corresponding detail pane. Without the permission: • The **Observable** and the **Entity** tabs display an error message with a **403 Forbidden** HTTP status code. • The observable and the entity rule detail panes ares not available.
read sources	Enables viewing the list of allowed sources for groups, entities, and observables.	With the permission: • Users can view the list of **Allowed sources** in group detail panes. • Users can view the **Sources** summary information in the **Groups** view. • Users can view the list of entity and observable sources in entity and observable detail panes, under **Sources**. Without the permission: • In the **Groups** view, no source information is available under the **Sources** column header. • The **Sources** section is not available in entity and observable detail panes.

Permission	Purpose	Behavior in the platform
read tasks	Enables viewing system jobs.	With the permission: • In the left navigation bar users can click ⚙ , **System** jobs to view lists of platform system jobs. • Users can click one of the following tabs to view system jobs by status: ◦ **Running** ◦ **Succeeded** ◦ **Failed** ◦ **Revoked** • Users can click a job on the list to display the corresponding detail pane with more information. Without the permission: • The **System jobs** menu option is not available in the ⚙ pop-up menu. • The **System jobs** view and the corresponding tabs are not available. • The system job detail pane is not available.

Permission	Purpose	Behavior in the platform
read taxii-services	Enables viewing TAXII services.	With the permission: • Users can view global STIX and TAXII configuration settings for the platform. • Users can access the **STIX** and **TAXII** options by clicking ⚙, and then **System settings** in the left navigation bar. Without this permission: • Users cannot view global STIX and TAXII configuration settings. • The **STIX** and **TAXII** views display an error message with a **403 Forbidden HTTP** status code.
read taxonomies	Enables viewing the taxonomy list.	With the permission: • Users can view a list with all existing taxonomy tags in the **Taxonomies** view. • If an entity or an observable includes tags, users can view them in the corresponding entity or observable detail pane under **Tags**. Without the permission: • The **Taxonomies** view is not available in the top navigation bar. • Entity and observable detail panes do not include any details about tags.

Permission	Purpose	Behavior in the platform
read ticket-comments	Enables viewing comments to user tasks in workspaces, and in the **Tasks** view. ⓘ To work as expected, this permission requires the following permissions as dependencies: • read tickets	With the permission: • Users can view comments to existing user tasks in the task detail pane. • Users can view comments to user tasks in the following platform areas: ◦ Workspaces[53] ◦ **Tasks** Without the permission: • The **Comments** section in a task detail pane is not available.
read tickets	Enables viewing user tasks in workspaces, and in the **Tasks** view. ⓘ The following permissions require **read tickets** as a dependency to work as expected: • **read ticket-comments**	With the permission: • Users can view user tasks and task information in the task detail pane such as task owners and stakeholders, as well as deadlines and status. • Users can view user tasks in the following platform areas: ◦ Workspaces[54] ◦ **Tasks** Without the permission: • Users cannot create or modify user tasks. • The **Tasks** view, is not available. • The task detail pane is not available. • The option in the left navigation bar and the **My tasks** view are not available.

53 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces
54 https://docs.eclecticiq.com/get-to-know-the-platform/workspaces

Permission	Purpose	Behavior in the platform
read traceback-logs	Enables viewing traceback logs in the GUI.	With the permission: • Users can access and view traceback logs recording execution events and errors. • Task execution traceback logs are helpful when troubleshooting failed feed, enricher, rule, and upload actions. Without the permission: • Traceback logs are not available in the detail panes of feed, enricher, rules, and manually uploaded files when task runs result in a failed status.
read transports	Enables viewing available transport types for incoming and outgoing feeds.	With the permission: • Users can view incoming and outgoing feed transport types listed under **Transport** type in the **Incoming feeds** and the **Outgoing feeds** views. • Users can view incoming and outgoing feed transport types in the detail pane of a selected feed. Without the permission: • Incoming and outgoing feed transport type information is not available under **Transport** type in the **Incoming feeds** and the **Outgoing feeds** views. • Incoming and outgoing feed transport type information is not available in the detail pane of a selected feed.

Permission	Purpose	Behavior in the platform
read users	Enables viewing lists with users and their account details. ⓘ The following permissions require **read users** as a dependency to work as expected: • **modify groups** • **modify roles** • **read groups** • **read permissions** • **read roles**	With the permission: • User can access and view **User management** by clicking ⚙, **User management** in the left navigation bar. • Users can view workspace collaborators. • Users can view owners and stakeholders in user task detail panes. • Users can view users belonging to a group in the **Users** tab of the group detail pane. Without the permission: • The **User management** view and its tabs are not available. • It is not possible to view workspace collaborators. • It is not possible to view owners and stakeholders in user task detail panes. • It is not possible to view users belonging to a group in the **Users** tab of the group detail pane.

Permission	Purpose	Behavior in the platform
read workspace-comments	Enables viewing comments to workspaces users own or collaborate to. ⓘ To work as expected, this permission requires the following permissions as dependencies: • **read workspaces**	With the permission: • After opening a workspace, users can access the **Comments** view, and they can read workspace comments. Without the permission: • After opening a workspace, the **Comments** view is not available. • Attempts to directly access the **Comments** view by copy-pasting the corresponding URL into the browser address bar return a **401 Unauthorized** HTTP status code.

Permission	Purpose	Behavior in the platform
read workspaces	Enables viewing workspaces. ⓘ The following permissions require **read workspaces** as a dependency to work as expected: • **read workspace-comments**	With the permission: • Workspace collaborators can view listed workspaces and workspaces they belong to. • In the **Workspaces** view, users can click available workspaces to open and view them. • When users create or edit a dataset, they can assign it to one or more workspaces by selecting them from the **Workspaces** drop-down menu. • When users create or edit a user task, they can assign it to one or more workspaces by selecting them from the **Workspaces** drop-down menu. Without the permission: • The **Workspaces** option view, as well as the corresponding option in the top navigation bar, are not available. • When users create or edit a dataset, they cannot assign it to any workspaces. • When users create or edit a user task, they cannot assign it to any workspaces.

Permission	Purpose	Behavior in the platform
reset password	Enables resetting a user password.	With the permission: • In the sign-in view, users can click **Reset password** to trigger an email notification with instructions to reset and change a user password. • It is possible to reset and to change only the password associated with your own user profile. • Platform administrators can force password resetting on other user profiles than their own. Without the permission: • In the sign-in view, **Reset password** is not available. • Users cannot reset their password.

Data ingestion and dissemination

This feature set helps manage data streams and workflows to ingest, process, organize, and distribute intelligence to internal and external parties.

It is a data processing pipeline that allows daisy-chaining intelligence data-centered tasks and activities as part of the data ingestion process into the system.
The pipeline executes processing activities in an asynchronous manner, and it allows the system to manage and to distribute the activities across the available resources.

Data and intelligence sources: integrated products

Integrated products	Description
Anubis Cyberfeed	Provides information on DNS sinkholes and hits when a recursive DNS server queries for a bad domain name. Provides information on compromised machines and DNS servers, as well as compromised web sites and malware files.
AlienVault OpenThreat Exchange	OTX provides open access to a global community of threat researchers and security professionals. It now has more than 100,000 participants in 140 countries, who contribute over 19 million threat indicators daily. It delivers community-generated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques, strengthening your defenses while helping others do the same.
BFK	BFK is the field of malware analysis and incident response since 1990. It offers threat intel feeds, passive DNS, and enrichment APIs, that make use of up-to-date collection of static and dynamic sample analysis. The company's prime focus is crime-ware and APT attacks.
Binary Defense Systems Artillery Threat Intelligence Feed	A feed listing thousands of malicious IP addresses to block.
Bitdefender Advanced Threat Intelligence	Bitdefender Advanced Threat Intelligence feeds ingest: • Domain indicators related to APTs, malware, and phishing. • File hash indicators related to APTs. • IP address and C2 indicators related to APTs and IP addresses of connections to malicious C2 domains.
BitSight Anubis Cyberfeed	AnubisNetworks Cyberfeed allows customers to obtain threat intelligence on real-time security events, with monitoring of countries, organizations, and their subsidiaries.
Censys	Censys is an Internet-wide scanning system and database that aims at listing all devices and networks that compose the Internet, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configures and deployed.

Integrated products	Description
CentralOps	The CentalOps Domain Dossier enriches supported observables with a broad range of contextual information such as related country and city, ASN and network operator, registrar and whois.
CIRCL Passive SSL	CIRCL Passive SSL is a database storing historical X.509 certificates seen per IP address. The Passive SSL historical data is indexed per IP address, which makes it searchable for incident handlers, security analysts, or researchers. The Passive SSL enricher will retrieve domains and IPs associated with an SSL Certificate has.
Cisco Systems	The Cisco Umbrella API helps analysts quickly understand registration details, similar domains and potential malicious ties to observable data. With this integration, analysts can quickly discern threats and attribution intelligence from observables used in active campaigns as the cloud-based enricher provides information relating domains, IP addresses and file hashes. Combining this integration with EclecticIQ Platform enables analysts to dynamically build a repository of intelligence relating to domain activity.
Cofense PhishMe	Cofense PhishMe is the leading provider of human-driven phishing defense solutions worldwide. Our collective defense suite combines best-in class incident response technologies with timely attack intelligence sourced from employees. Cofense enables thousands of global organizations to stop attacks in progress faster and stay ahead of breaches..
Common Vulnerabilities and Exposures (CVE)	Enrich intelligence with exploit target information, from the standard source of vulnerabilities and exposures: the MITRE corporation. The enricher and feed uses the Computer Incident Response Center Luxembourg (CIRCL) CVE-search API to retrieve all the available details.

Integrated products	Description
Crowdstrike Falcon Threat Intelligence	Crowdstrike is a global leader in the cloud-delivered next-generation endpoint protection. With a single lightweight agent, CrowdStrike is the first company to unify next-generation antivirus that includes machine learning and behavioral analytics, endpoint detection and response (EDR), and a 24/7 managed hunting service all in one lightweight agent. Falcon IntelligenceTM is a cost-effective program tailored to each company's needs and requirements and addresses the legal and technical aspects of preventing harm that results from a cyberattack.
CVE Search	Enriches observables with information about common software and hardware vulnerabilities, along with the corresponding exposures. The enricher contacts the Computer Incident Response Center Luxembourg (CIRCL) cve-search API to retrieve all the available details associated with the input CVE IDs. CVE information about common software and hardware vulnerabilities, along with the corresponding exposures, is stored in the platform as enrichment observables.
CyberCrime Tracker ATM Provider CyberCrime Tracker Domain Provider CyberCrime Tracker Zbot Provider	CyberCrime trackers provide information about Command and Control (C2) systems that manage in the wild botnets.
Cybereason	Cybereason Deep Detect & Respond (EDR) helps you confidently answer the question "Are you under attack?" and defend against even the most advanced attacks. The integration with EclecticIQ Platform aims at further enabling Cybereason's solution with Threat Intelligence, providing indicators of compromise (MD5 hashes, domain names and IP addresses) from Third Party vendors, as well as in-house Threat Intelligence Analysts, after having been curated through the platform. Cybereason operations teams do not need to learn working with a new tool and can focus on providing timely response actions to their internal customers. For EclecticIQ Platform users, this is business as usual: disseminating IOCs for consumption by security controls.
Cybersprint	Cybersprint protects organizations from cyber threats by providing real-time insights into their online footprint and their current digital risks.

Integrated products	Description
Digital Shadows Searchlight Global Incidents Provider Digital Shadows Searchlight Private Incidents Provider	Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface. Digital Shadows Searchlight enables proactive monitoring of the organization's assets and resources against malicious actors and activities that could target the organization.
DomainTools	DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network and connect them with nearly every active domain on the Internet. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and migration work.
Dragos	As a leading provider of industrial control systems cybersecurity, the Dragos threat detection and response platform codifies decades of real-world experience in advanced threat analytics. It provides operational and information technology practitioners unprecedented visibility and prescriptive procedures to respond to adversaries in the industrial threat landscape. Through the integration with EclecticIQ Platform, Threat Intelligence Analysts now have access to relevant reports, Indicators, Threat Actors, TTPs and observables that Dragos provides for this unique threat landscape.
DShield	DShield is a community-based collaborative firewall log correlation system to analyze attack trends worldwide.
EclecticIQ Commercial Sources Feed	EclecticIQ Commercial Sources Feed is the commercial intelligence feed curated by the EclecticIQ Fusion Center team.
EclecticIQ Open Sources Feed	EclecticIQ Open Sources Feed is an open source intelligence feed curated by the EclecticIQ Fusion Center team.
Elasticsearch	Elasticsearch sightings searches for an external Elasticsearch instance. Any hits matching the search criteria are processed to automatically generate corresponding sightings.

Integrated products	Description
Farsight Security DNSDB	Farsight Security DNSDB is a Passive DNS historical database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DSN experts.
FireEye iSIGHT Intelligence	FireEye iSIGHT Intelligence is a proactive, forward-looking means of qualifying threats poised to disrupt your business based on the intents, tools, and tactics of the attacker. Our high-fidelity, comprehensive intelligence delivers visibility beyond the typical attack lifecycle, adding context and priority to global threats before, during, and after an attack. It helps mitigate risk, bolster incident response, and enhance your overall security ecosystem.
Flashpoint	Flashpoint is the market leader in threat intelligence from the Deep and Dark Web. Flashpoint's products illuminate threatening actors, relationships, behaviors, and networks.
Forcepoint Email Security Forcepoint Web Security	Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people’s behaviors and intent as they interact with critical data and IP wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to data while protecting intellectual property and simplifying compliance.
Fox-IT InTELL	InTELL tracks global criminal activity with intelligence based on actor attribution and context. Going beyond botnet and malware information, InTELL provides a global picture of trends, geographical activity, actors, their motivations, and their evolving business models. Real-time contextual cyber intelligence includes global visibility on actor trends, threats and technology; tracking of risks, and threats to online brads; and contextual threat feeds.
FS-ISAC	The Financial Services Information Sharing and Analysis Center is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions around the globe and in turn their customers, the organization leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyberthreats.
Group-IB Threat Intelligence	Group-IB is a global provider of security services and threat intelligence solutions with profound expertise providing the global security community insights into Russian-speaking cyber criminal groups and their tactics.

Integrated products	Description
Hail a TAXII	Hail a TAXII.com is a repository of Open Source Cyber Threat Intelligence feeds in STIX format. There are currently 1107066 indicators.
Honeypot.dk	Honeypot.dk offers a number of industrial control systems (ICS) and SCADA (Supervisory Control and Data Acquisition) threat feeds in the following industries: energy, transportation, healthcare, water and waste water management, as well as other types of industrial manufacturing. This niche supplier is a must have when it comes to securing critical infrastructure sectors, which support our everyday lives. The integration with EclecticIQ Platform allows to ingest these threat feeds and convert them into relevant TTPs, attack patterns, and Indicators, enabling the analyst to build actionable threat intelligence with a real-life perspective.
HybridAnalysis	HybridAnalysis is a free malware analysis service providing in-depth static and dynamic analysis of submitted files.
Infoblox	Infoblox DDI / NIOS (Network Identity Operating System) automates the error-prone and time-consuming manual tasks associated with deploying and managing DNS, DHCP, and IP address management (IPAM) required for continuous IP network availability and business uptime. The integration with EclecticIQ Platform aims at further enabling Infoblox' solution with Threat Intelligence, providing indicators of compromise (domains, IP addresses) from Third Party vendors, as well as in-house Threat Intelligence Analysts, after having been curated through the platform. Infoblox operations teams do not need to learn working with a new tool and can focus on providing timely response actions to their internal customers. For EclecticIQ Platform users, this is business as usual: disseminating IOCs for consumption by security controls.
IntSights Alerts	IntSights Alerts produce information gathered from the dark web. This integration focuses on brand reputation protection, as well as fraud and phishing prevention.

Integrated products	Description
Intel 471 Adversary Intelligence	Intel 471's Adversary Intelligence is focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks. This includes a globally dispersed intelligence collection function partnered with a headquartered based intelligence analysis function that produces various finished intelligence products. The integration with EclecticIQ Platform allow to work with Intel 471 Threat Intelligence Data through a feed of reports and indicators, as well as an enricher, covering a wide variety of observable types.
Intel 471 Malware Intelligence	Intel 471's Malware Intelligence provides high fidelity and timely indicators with rich context. It enables organizations to immediately block and gain understanding of crime ware campaigns as soon as cybercriminals carry out attacks. This intelligence aids threat detection, incident response, hunting, as well as threat intelligence uses cases within SOCs, security, and incident response teams. EclecticIQ Platform integration supports the ingestion of Malware intelligence reports, TTP information, file and network-bases Indicators, all mapped to MITRE ATT&CK.
Intel McAfee DXL/MAR/TIE	The McAfee Active Response (MAR) integration provides enrichment capabilities which allows user to run live lookups based on MD5 hashes and create new observables. McAfee Threat Intelligence Exchange (TIE) acts as a broker that combines intelligence from local security solutions. With this integration, EclecticIQ Platform users can query McAfee TIE and ingest and leverage this intelligence in their threat analysis workflows.
JoeSandbox Analysis Feed	Ingests analysis reports as TTP entities, and related artifacts found during analysis as indicator entities. It produces: • TTP entities for each analysis report. • Indicator entities for each artifact related to the report. • Observables for each indicator of compromise identified for found artifacts.

Integrated products	Description
Kaspersky Threat Intelligence Data Feed	Kaspersky Lab offers continuously updated Threat Data Feeds to detect malicious activity on your enterprise network. Threat Intelligence is aggregated from fused, heterogeneous and highly reliable sources such as Kaspersky Security Network and web crawlers, Botnet Monitoring service, spam traps, research teams, the deep web, partners and other historical data about malicious objects collected by Kaspersky Lab over 2 decades. This integration enables the Threat Intelligence Analyst to leverage a wealth of Threat Intelligence data, including TTPs, Indicators and Observables (via the URL and IP Address feeds) within multiple categories of interest, such as ransomware, phishing, malicious URLs, IP reputation, malicious files and trojans for mobile, and botnet.
Kaspersky Threat Intelligence Portal	Integration with Kaspersky Lab Threat Intelligence Portal lets users have immediate access to the latest and historical threat intelligence. The Portal provides analysts with a single point of entry to 3 essential Kaspersky products: the Kaspersky Threat Lookup, APT and Financial Reports, along with Threat Intelligence Data Feeds. Analysts have continuously updated threat intelligence including TTPs, Indicators, and Observables, within multiple categories of interest at their fingertips.
Malwaredomains	The DNS-BH project creates and maintains a listing of domains that are known to be used to propagate malware and spyware.
MaxMind GeoIP	MaxMind is an industry-leading provider of IP intelligence. ElecticIQ Platform users can leverage GeoIP databases to enrich and develop context on their IP feeds.
MicroFocus ArcSight	Micro Focus ArcSight is a cyber security product, first released in 2000, that provides big data security analytics and intelligence software for security information and event management (SIEM) and log management. ArcSight is designed to help customers identify and prioritize security threats, organize and track incident response activities, and simplify audit and compliance activities.
Microsoft Sentinel Alerts	Microsoft Sentinel Alerts ingests security alerts from a predefined Microsoft Azure Log Analytics workspace.
MISP	MISP is an open source platform that allows for easy IOC sharing among distinct organizations. With this MISP integration, threat analysts can ingest the IOCs they receive from MISP and apply their threat investigation and dissemination workflows right from EclecticIQ Platform.

Integrated products	Description
NCFTA ListServ Intel	The National Cyber-Forensics and Training Alliance (NCFTA) is a non-profit partnership between private industry, government, and academia providing a neutral and trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cybercrime. They provide information on various threat actors, collected via various ListServ systems. Their CyFin ListServ data corpus focuses on crimes and cyber schemes targeting the financial sector, such as stock manipulation, electronic funds transfer fraud, use of money mule networks, and the use and abuse of a growing number of telecommunication utilities (mobile banking, SMS texting).
NSFocus	The integration of NSFocus Global Intelligence includes both the feed and enricher. NSFocus Threat Intelligence with its extensive sources, provides analysts with enricher information for IP addresses, Domains, CVEs, and files. The NSFocus API allows analysts to work with the security event data as a feed. The cyber threat landscape in China is larger and more complex than anywhere else. With this integration, analysts have insight into the world's largest numbers of Internet-connected devices and vast numbers of Internet users.
OpenPhish	OpenPhish offers a platform for phishing intelligence, identifies phishing sites and performs intelligence analysis in real time.
OpenResolve	OpenResolve by Cisco OpenDNS offers a REST API to use DNS resolvers and to retrieve reverse-DNS lookup information.
Palo Alto Auto Focus Threat Intelligence	Gain visibility into the most critical threats with contextual intelligence on malware families, campaigns, threat actors, malicious behaviors and exploits used. AutoFocus allows you to answer questions like: “Who is attacking me?” “What tools are they using?” and “How targeted or unique is this threat?”
Palo Alto PAN-OS	PAN-OS incoming feeds ingest PAN-OS traffic logs to generate and report sightings.

Integrated products	Description
PassiveTotal	PassiveTotal enrichers provide additional context to augment queried IP addresses, domain names, whois, and malware. Based on the input observable types, PassiveTotal enrichers return additional contextual information such as sub-domains, inet details, autonomous system number (ASN), and geolocation details; historical information to cross-reference IP addresses to the corresponding DNS domain names over time; whois lookup information such as registrar, organization, country, city, street, telephone, and email details; malware hash and collection date.
PhishTank	PhishTank is a free community site to submit and to verify phishing data.
Proofpoint	Proofpoint is an enterprise security company that provides security and compliance solutions.
PyDat	The PyDat enricher provides whois, including historical whois, and passive DNS lookup information. PyDat is installed locally, and it can work together with an Elasticsearch instance to provide whois, including historical whois, and passive DNS lookup information. Analysts can use it to retrieve names, organizations, countries, cities, street-names, ZIP codes, telephone-numbers, and email details.
Recorded Future	The Recorded Future integration provides both a feed and enricher capabilities. With the feed, users have access to the Recorded Future Risk List, which includes IP and file hashes, for example. The results are provided in standard STIX/TAXII protocols, including TTPs and Indicators. The enricher allows users to query Domains, hashes, URLs, and IP addresses.
RIPEstat	RIPEstat provides everything you ever wanted to know about IP address space, Autonomous System Numbers (ASNs), and related information for hostnames and countries in one place.
RiskIQ Passive Total	RiskIQ PassiveTotal overcomes the challenges in discovering and proactively blocking malicious infrastructure. Using innovative techniques and research processes, PassiveTotal provides analysts with a single view into all the data they need.

Integrated products	Description
RSA NetWitness RSA Secure Analytics	Using the NetWitness app, RSA users are able to leverage the power of EclecticIQ Platform directly from the NetWitness interface. Users can receive IOCs from EclecticIQ Platform to trigger security alerts, and send sightings back to EclecticIQ Platform.
SenseCy	SenseCy (a Verint Company) is a leading Israeli provider of actionable Cyber Threat Intelligence (CTI) solutions, relying on a unique Virtual HUMINT-based methodology that combines highly skilled analysts with advanced domain expertise and proficiency in over 15 languages, and the most advanced Web Intelligence (WEBINT) systems on the market by Verint, providing multiple platforms for the automatic collection and analysis of Actionable Intelligence® from the entire web.
Shodan	Shodan is the world's first search engine for Internet-connected devices. The Shodan enricher rakes 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.
Silobreaker	Uses the Silobreaker In Focus API to enrich supported observables with analysis and other observables with intelligence from the Silobreaker Online platform. Enriching an observable on the EclecticIQ Platform attaches a Silobreaker In Focus Cyber report entity to it, along with related observables.
Splunk	Based on the search queries defined in the enricher, the enricher looks for matching data in the specified Splunk instance. Matching data is extracted and saved to the platform as sightings.

Integrated products	Description
Splunk Phantom	Phantom is a security orchestration platform. It is designed to act as the glue that binds all the security tools in an Organisation together. Security Orchestration tools are designed to use security orchestration plugins to interact with the security tool using the security tools native functionality. Meaning that the Phantom integration is the opposite from normal integrations. No plugin for the EclecticIQ Analyst Platform is created. Instead an EclecticIQ Phantom App for the Phantom Security Orchestration tool is created. The EclecticIQ Phantom App interacts with EclecticIQ Platform, allowing the Phantom Security Orchestration tool to request information from EclecticIQ Platform, and process process received information. This integration enables Phantom users to benefit from the wealth of threat intelligence data available within the EclecticIQ Platform, without leaving the Phantom interface.
Spycloud	The SpyCloud integration feed helps users protect employees and customers. It provides information which can prevent account take over, fraud IP theft, and brand damage. The feed alerts users when an employee's or company's assets have been compromised.
Symantec DeepSight Intelligence	Leveraging the extensive Symantec Global Intelligence Network, this integration feed allows users to collect raw intelligence data making it available within EclecticIQ Platform. The feed provides a broad range of insights, covering reputation and threat intelligence data for IP, URLs, attacks, bots, cnc, malware, fraud, and phishing.
TAXII 1.0, 1.1, 2.1	TAXII (Trusted Automated eXchange of Indicator Information) is a collection of services and message exchanges to enable the sharing of information about cyber threats across product, service and organizational boundaries. It is a transport vehicle for STIX structured threat information and key enabler to widespread exchange.
Threat Recon	Threat Recon is a cyber threat indicator search engine.

Integrated products	Description
ThreatCrowd	ThreatCrowd is an Open Source system for finding and researching artefacts relating to cyber threats, utilizing information obtained by crawling various Open Source resources, including VirusTotal and Malwr. ThreatCrowd is an Open Source system for dinging and researching artefacts relating to cyber threats, utilizing information obtained by crawling various Open Source resources, including VirusTotal and Malwr.
Unshorten URL	Is that short URL you're visiting REALLY going to contain cute kittens, or instead is it going to mug you and steal your wallet? Unshorten.It! takes any bullets for you, analysing the website for safety and letting you see it before you decide whether to proceed.
VirusTotal Private Mass API	With VirusTotal, users can analyze suspicious files and URLs. It facilitates the quick identification of viruses, worms, trojans, and all kinds of malware. Integrating VirusTotal means that users don't need to leave EclecticIQ Platform - everything is at your fingertips which saves time and minimizes the number of tools open at once. The integration supports the premium service for feeds and enrichers; plus, the free service for enrichers. VirusTotal helps users by providing more condenses, ingestible, and corroborable information.
VMRay Malware Submission	VMRay Malware Submission Feed ingests malware samples and submissions from a VMRay instance. Malware submissions are ingested to the platform as TTP entities, whereas malware samples are ingested as indicators.
Wapack Labs Threat Recon	Wapack Labs identifies cyber threats before they become attacks, providing threat detection through internet surveillance operations, data gathering, and in-depth analysis of economic, financial, and geopolitical issues.
Web Browser plugins (Google Chrome and Mozilla Firefox)	With EclecticIQ CTI Clipboard, users can stay in their browser (Google Chrome) when copying/pasting information. Users are able to focus on the investigation at hand, without the need to switch between tabs/platforms. This time saving application allows users to create indicators within the CTI Clipboard extension itself, which are directly taken into EclecticIQ Platform.
Webroot BrightCloud Threat Intelligence	Enriches ipv4, hash-md5, domain and uri observables with Webroot BrightCloud Threat Intelligence to add historical data and related intelligence.

Integrated products	Description
Zscaler	Zscaler Outgoing Feed publishes supported observables to a URL category on Zscaler Internet Access (ZIA), which you can then apply URL filtering rules to.

Generic transport types

Source	Supported incoming feeds	Description
FTP	download	These transport types enable data exchange: • In networked data stores in a LAN (mount point) • Among external servers or data repositories in a LAN or WAN (FTP, HTTP, SFTP) • By email (IMAP) • By RSS feed (RSS).
HTTP	download	
IMAP	email attachment fetcher email fetcher	
Mount point	download	
RSS	RSS version 2.0	
SFTP	SFTP download	
TAXII 1.0	download	
TAXII 2.1	download	

Content types for generic outgoing data

The next table describes the generic transport types available for outgoing feeds, and the content types supported:

Transport type	ArcSight CEF	EclecticIQ Entities CSV	EclecticIQ Observables CSV	EclecticIQ HTML Report	EclecticIQ HTML Report Digest	EclecticIQ JSON	Plain text	STIX 1.2	STIX 2.1	PAN-OS External Dynamic List
Amazon S3 push	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Email	✓	✓	✓	✓	✓	✓	✓	✓	✓	
FTP upload	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HTTP download	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mount point upload	✓	✓	✓	✓	✓	✓	✓	✓	✓	
SFTP upload	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Syslog push	✓	✓	✓						✓	
TAXII inbox (v1.0, v2.1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAXII poll (v1.0)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Supported TAXII services

After configuring a TAXII server, you can set up TAXII services.

A TAXII service is a specialized data handler that implements a specific TAXII capability.

The platform supports the following TAXII services:

Service type	Description
Collection management service	You can use a TAXII collection management service to: • Request information about TAXII data collections. • Subscribe to TAXII data collections. • Cancel subscriptions to TAXII data collections. You can poll a TAXII collection to: • Obtain overviews of the available content. • Check for updated content. • Select TAXII feeds and datasets to use as data sources. TAXII data collections — structured TAXII data feeds, and unstructured TAXII datasets — are examples of TAXII inbox and TAXII poll service content. Bindings: • TAXII HTTP 1.0 • TAXII HTTPS 1.0
Discovery service	You can use a TAXII discovery service to obtain information about the availability and the use of TAXII services such as collection management, inbox, and polling. Bindings: • TAXII HTTP 1.0 • TAXII HTTPS 1.0

Service type	Description
Inbox service	The TAXII inbox service enables data producers to initiate push messages to service consumers. This service can be based on a subscription model, or it can be an unsolicited payload a producer pushes to a consumer. Bindings: • TAXII HTTP 1.0 • TAXII HTTPS 1.0
Poll service	The TAXII poll service enables consumers to request TAXII data collection content from a TAXII producer, usually through TAXII outgoing feeds. Bindings: • TAXII HTTP 1.0 • TAXII HTTPS 1.0

Third-party applications

We provide integrations with the following third-party vendors that allow you to interact with their services using your EclecticIQ Platform instance.

Third-party vendor/software	Integrations
Micro Focus ArcSight ESM	• ArcSight Smart Connector • EclecticIQ base content package For more information, see the documentation[55].
IBM QRadar	• Threat Intelligence EclecticIQ Platform App[56] for IBM QRadar For more information, see the documentation[57].

55 https://docs.eclecticiq.com/integrations/apps/micro-focus-arcsight-esm
56 https://exchange.xforce.ibmcloud.com/hub/extension/680e595aac8080e2acbc556b29c585f4
57 https://docs.eclecticiq.com/integrations/apps/integrate-with-ibm-qradar

Third-party vendor/software	Integrations
Splunk	• Threat Intelligence EclecticIQ Platform App[58] for Splunk. For more information, see the documentation[59].
Splunk Phantom	• EclecticIQ App[60] for Splunk Phantom For more information, see: • the EclecticIQ App reference[61]. • the documentation[62].
MISP	• MISP incoming feed[63] • MISP outgoing feed[64]
EclecticIQ browser extension	Available on: • FireFox[65] • Chrome[66] For more information, see the documentation[67].

Data management policies

Data policies help define data retention criteria for incoming data that is ingested and stored in the platform.

Entities and observables matching the specified policy criteria are deleted when their retention period expires.

The process removes also any relationships that may be left dangling after removing entities and observables with relationships.

58 https://splunkbase.splunk.com/app/4176/
59 https://docs.eclecticiq.com/integrations/apps/splunk
60 https://my.phantom.us/4.10/apps/
61 https://my.phantom.us/4.10/docs/app_reference/phantom_eclecticiqapp
62 https://docs.eclecticiq.com/integrations/apps/splunk-phantom
63 https://docs.eclecticiq.com/integrations/extensions/incoming-feeds/list-of-incoming-feeds/incoming-feed-misp
64 https://docs.eclecticiq.com/integrations/extensions/outgoing-feeds/list-of-outgoing-feeds/outgoing-feed-misp
65 https://addons.mozilla.org/en-US/firefox/addon/eclecticiq/
66 https://chrome.google.com/webstore/detail/eclecticiq/palpgaigcadbokempolkolbjjolmogoh
67 https://docs.eclecticiq.com/integrations/eclecticiq-browser-extension/getting-started

This approach enables setting up rules to handle ingested data, so that it complies with applicable norms and regulations concerning fair data management and privacy.

For example, GDPR-compliant countries enforce specific criteria to control data retention and PII data usage.

User Interfaces

GUI

The platform offers a web-based graphical user interface.

- Minimum screen resolution is 1280x720.
- Recommended screen resolution: 1920x1080.

EclecticIQ Platform web-based GUI fully supports the latest/current versions of the following web browsers:

- Google Chrome

EclecticIQ Platform web-based GUI functionally supports the latest/current versions of the following web browsers:

- Microsoft Edge
- Mozilla Firefox
- Microsoft Internet Explorer 11
- Opera
- Apple Safari

API

API-integrations enable platform interoperability with third-party products to expand platform functionality in a modular way.

You can integrate the platform with upstream products that make intelligence available for ingestion and analysis, as well as with downstream products that can consume intelligence they receive from the platform.

- The standard way to integrate a data source or a data provider with the platform is through incoming feeds and enrichers:

    - Incoming feeds enable ingesting intelligence that is processed and stored in the platform as entities and observables.
    - Enrichers enable ingesting intelligence that adds context information to existing entities and observables.
- To use the platform as a data source to disseminate intelligence, you can create outgoing feeds.
- You can also use a dedicated app to exchange observables and sightings between EclecticIQ Platform and a Splunk instance, as well as connect two platform instances to exchange intelligence information.

REST API endpoint	HTTP method	Permission
`/api/datasets/`	`GET`	**read intel-sets**
`/api/datasets/${int:id}`	`GET`	**read intel-sets**
`/api/enrichers/`	`GET`	**read enrichers**
`/api/enrichers/${int:id}`	`GET`	**read enrichers**
`/api/enrichment-tasks/${uuid:id}`	`GET`	**read tasks**
`/api/entities/`	`GET`	**read entities**
`/api/entities/`	`POST`	**modify entities**
`/api/entities/${uuid:id}`	`GET`	**read entities**
`/api/entities/${uuid:id}/enrich`	`POST`	**modify entities**
`/api/entities/${uuid:id}/enrichers`	`GET`	**read entities**
`/api/entities/latest`	`GET`	**read entities**
`/api/observables/`	`GET`	**read extracts**

REST API endpoint	HTTP method	Permission
`/api/observables/`	`POST`	**modify extracts**
`/api/observables/${int:id}`	`GET`	**read extracts**
`/api/observables/${int:id}`	`PATCH`	**modify extracts**
`/api/observables/${int:id}/enrich`	`POST`	**modify entities**
`/api/observables/${int:id}/enrichers`	`GET`	**read extracts**
`/api/sources/`	`GET`	**read sources**

SDK

Internal Python API

- **Intel fetcher API**
  Development of custom components that can obtain intel data from different, not natively supported, source types.
  This assumes an API supporting development of authentication and authorization sub-components.
- **Intel data transformer API**
  Development of custom data transformers that can transform incoming data into EclecticIQ entities.
- **Intel enrichers API**
  Development of custom intel enrichers that can query any external system asynchronously through APIs or other services the external systems expose, with the purpose of augmenting existing intel data or generating new data.
- **Outgoing feed composer API**
  Development of custom data composers that can transform existing intel data such as EclecticIQ entities to any target format.