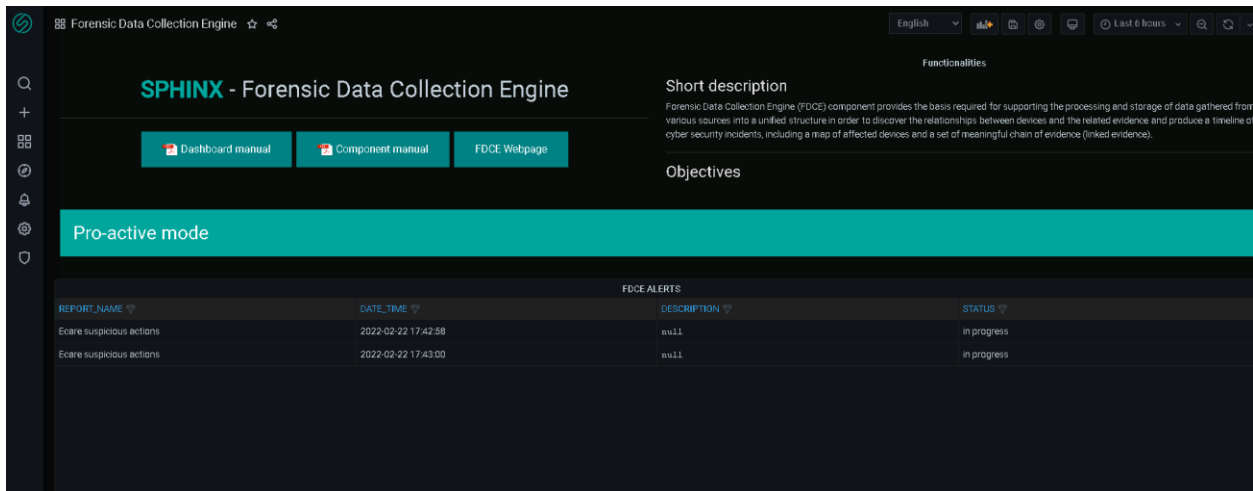


Forensic Data Collection Engine (FDCE) component provides the basis required for supporting the processing and storage of data gathered from various sources into a unified structure in order to discover the relationships between devices and the related evidence and produce a timeline of cyber security incidents, including a map of affected devices and a set of meaningful chain of evidence (linked evidence).

#### Visualisations:

- FDCE Alerts – containing new alerts raised by FDCE, which has draggable columns and filters;
- FDCE Report topic - containing data from another topic of FDCE, containing details about reports with draggable and filter columns;

#### Example for FDCE Alerts:



The screenshot displays the SPHINX - Forensic Data Collection Engine dashboard. The interface includes a sidebar with navigation icons, a top header with the application name and user information, and a main content area. The main content area features a 'Pro-active mode' banner and a table titled 'FDCE ALERTS'. The table has columns for 'REPORT\_NAME', 'DATE\_TIME', 'DESCRIPTION', and 'STATUS'. Two rows of data are visible, both with a status of 'in progress'.

| REPORT_NAME              | DATE_TIME           | DESCRIPTION | STATUS      |
|--------------------------|---------------------|-------------|-------------|
| Ecare suspicious actions | 2022-02-22 17:42:58 | null        | in progress |
| Ecare suspicious actions | 2022-02-22 17:43:00 | null        | in progress |