The SIEM component is responsible for triggering alerts and to match information using log files that are collected from multiple resources such as data collected from Data traffic monitoring, system log files, auditing checks, vulnerability assessments. The data can be either constructed data (json, csv files) or raw text files that can be converted to structured data by using regular expressions. The SIEM continuously monitors the events created from the log files and trigger the alerts.

Visualisations synchronised with the timerange:

- Low number of vulnerabilities which contains the rule_level field between 0 and 7;

- Medium number of vulnerabilities which contains the rule_level field between 8 and 10;

- High number of vulnerabilities which contains the rule_level field above 10;

- Internal vulnerabilities table;

- Certifications (containing detailed data about alerts) table.