Team: T10 TeamWork

Assignment: CRC

Due Date: 02/18/2020

Professor: Dr. Roach

**Classes, Responsibilities and Collaborations**

**1. Log File**

* Description: A file of any type (i.e. csv, jpeg, pdf, etc…) that has been ingested by the system.
* Responsibility 1: Knows its own file type, ingestion errors (if any exist), and all its own lof content.

2. **Log Entry**

* Description: Normalized data recovered from log files.
* Responsibility 1: Knows the attributes of Log Entry Number, Log Entry Timestamp, Log Entry Content, Host, and Source.

3. **Event Configuration**

* Description: Configuration for a project that determines the file paths and time restraints to place on log files to be ingested.
* Responsibility 1: Knows the root path of log files (1), file path of red team log files (1), file path of blue team log files (1), file path of white team log files (1), and time restraints on the log files (1).

4. **Vector**

* Description: Series of activities or steps that are necessary to achieve an object.
* Responsibility 1: Knows vector Name, and vector Description.
* Responsibility 2: Vector configuration has Add Vector, Delete vector, Edit vector, and a vector table.

5. **Graph**

* Description: A visual representation of a vector.
* Responsibility 1: Knows attributes of Orientation, Export Format, Interval Units, Interval, Position of Nodes, and Position of Relationships.
* Responsibility 2: A Graph contains at least one node (6).

6. **Node**

* Description: A visual representation of a significant event.
* Responsibility 1: Knows attributes of Node ID, Node Name, Node Timestamp, Node Description, Log Entry Reference (2), Log Creator, Event Type, Icon Type, Source, Node Visibility.
* Responsibility 2: A Node is part of at least one graph (5).
* Responsibility 3: Knows information about its relationships (9).

7. **Filter**

* Description: Used to display log entries that match the filter criteria.
* Responsibility 1: Narrows down log entry search results to those that match the filter criteria.
* Responsibility 2: Has access to log entry (2) data to match its filter criteria.

8. **Enforcement Action Report**

* Description: Contains error report information.
* Responsibility 1: Knows the attributes of Line Number and Error Message.
* Responsibility 2: Has access to log file (1) data to acquire Line Number error information.

9. **Relationship**

* Description: Establishes the association between parent and child node.
* Responsibility 1:Knows attributes of relationship ID, Parent ID, Child ID, and Label.
* Responsibility 2: Has access to a parent node (6) and a child node. (6)
* Responsibility 3: Has a describing label of the association.

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** main | |  |
| **Superclass:** None | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of handling transition to the project workspace | |  |
| **Responsibilities:**  1. Handle transitions to other windows. | **Collaborations:**  1. Handle transition to ProjectConfigWindow.  2. Handle transition to NavigatorWindow. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** ProjectConfigWindow | |  |
| **Superclass:** main | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of handling the validation and ingestion process. | |  |
| **Responsibilities:**  1. Retrieve directory path of log files  2. Handle event time range for the project.  3. Handle event name and description for the project.  4. Handle transition to ValidationIngestionWindow. | **Collaborations:**  1. Retrieve directory data from DirDialog.  2. Send directory data to ValidationIngestionWindow.  3. Send event date information to ValidationIngestionWindow. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** DirDialog | |  |
| **Superclass:** ProjectConfigWindow | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of handling directory path. | |  |
| **Responsibilities:**  1. Retrieve directory path of log files. | **Collaborations:**  1. Send directory path to ProjectConfigWindow. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** ValidationIngestionWindow | |  |
| **Superclass:** ProjectConfigWindow | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of handling the validation and ingestion process. | |  |
| **Responsibilities:**  1. Validate log file data.  2. Ingest log file data.  3. Handle log entries.  4. Handle transition to NavigatorWindow. | **Collaborations:**  1. Send log file data to Splunk. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** Splunk | |  |
| **Superclass:** ValidationIngestionWindow | |  |
| **Subclasses:** None | |  |
| **Description:** External software tool used in the creation of log entries. | |  |
| **Responsibilities:**  1. Transform log file data into log entries.  2. Archive log entries into a local database. | **Collaborations:**  1. Use MongoDB as the local database. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** MongoDB | |  |
| **Superclass:** NavigatorWindow | |  |
| **Subclasses:** None | |  |
| **Description:** External software tool used in the management of data. | |  |
| **Responsibilities:**  1. Store data from Splunk.  2. Handle data management being imposed by NavigatorWindow. | **Collaborations:**  1. Work with NavigatorWidow to exchange data. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** NavigatorWindow | |  |
| **Superclass:** ValidationIngestionWindow | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of log entry handling. | |  |
| **Responsibilities:**  1. Sort through log entry data.  2. Prepare data changes for MongoDB.  3. Create Vectors. | **Collaborations:**  1. Work with GraphTableWindow to exchange data.  2. Send data changes to MongoDB. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **Concrete Class:** GraphTableWindow | |  |
| **Superclass:** NavigatorWindow | |  |
| **Subclasses:** None | |  |
| **Description:** Window in charge of graphing log entry in vector format. | |  |
| **Responsibilities:**  1. Create vectors.  2. Show graphical representation of vectors.  3. Show table representation of vectors.  4. Edit graphical representation of vectors.  5. Edit table representation of vectors.  6. Create relationships among nodes.  7. Create nodes. | **Collaborations:**  1. Work with NavigatorWindow to exchange data.  2. Send data changes to MongoDB. |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |