Classes, Responsibilities and Collaborations

1. Event
   1. Responsibilities:
      1. Knows:
         1. Event Name
         2. Event Description
         3. Event Start Timestamp
         4. Event End Timestamp
         5. Root Directory
         6. Red Team Folder
         7. White Team Folder
         8. Blue Team Folder
         9. Lead
         10. Lead’s IP Address
         11. Connection to the host machine
      2. Can:
         1. Check connection to lead conditions are true:
            1. Lead’s checkbox is unchecked
            2. Lead’s IP address is not empty
            3. The IP address of the local machine is not the same as lead’s IP address
         2. Display error for any undesired action for connection to lead conditions
         3. Structural check operation:
            1. The root directory shall contain three folders
            2. The names of the three folders shall match the red team folder name, blue team folder name, and white team folder name specified in the event configuration
            3. The name of the root directory shall not be editable once the event is saved
         4. Generate a root directory structure error
         5. Perform the data cleansing operation
   2. Collaborators:
      1. none
2. Log File
   1. Responsibilities:
      1. Knows:
         1. Log File Name
         2. Cleansing Status
         3. Validation Status
         4. Ingestion Status
         5. Acknowledgment status
         6. Cleansed Log Files in permanent storage
         7. Significant Log Entries in permanent storage
      2. Can:
         1. Data transformation operation of a log file
         2. Data cleansing operation of log file
         3. Data validation operation of log file
         4. Perform the data ingestion operation once data ingestion operation is complete
         5. Update ingested log file
         6. Do search operation by keyword
         7. Do different search mechanisms
            1. Logical searching
            2. Wildcard searching
   2. Collaborators:
      1. Gets log data based on the Event Configuration settings.
3. Enforcement Action Report
   1. Responsibilities:
      1. Knows:
         1. Line Number
         2. Error Message
      2. Can:
         1. Generate an enforcement action report and set the validation status of the log file to “fail” of data validation fails
         2. Certify the cleansed log file as validated log file once verification action confirmation is received
         3. Display the line numbers and error messages pertaining to the selected log file in the enforcement action table
   2. Collaborators:
      1. Receives data from Log File for error handling and reports.
4. Vector
   1. Responsibilities:
      1. Knows:
         1. Vector Name
         2. Vector Description
         3. At least one significant entry
      2. Can:
         1. Save the changes to permanent storage
         2. Enable the user to edit the selected log entry
         3. Add significant log entries to a vector
         4. Establish connection between the lead and the user
         5. Allow user to do “Pull” operation
         6. Allow user to do “Push” operation
   2. Collaborators:
      1. Gets logs from Significant Log Entries.
5. Significant Log Entry
   1. Responsibilities:
      1. Knows:
         1. Log Entry Number
         2. Log Entry Timestamp
         3. Log Entry Content
         4. Host
         5. Source
         6. Source Type
         7. At least one vector
      2. Can:
         1. Mark a log entry as significant or not
         2. Add significant log entry to a vector
   2. Collaborators:
      1. Created from data from Log File
6. Node
   1. Responsibilities:
      1. Knows:
         1. Node ID
         2. Node Name
         3. Node Timestamp
         4. Node Description
         5. Log Entry Reference
         6. Log Creator
         7. Event Type
         8. Icon Type
         9. Source
         10. Node Visibility
         11. At least one graph
         12. Node Id Visibility
         13. Node Name Visibility
         14. Node Timestamp Visibility
         15. Node Description Visibility
         16. Log Entry Reference Visibility
         17. Log Creator Visibility
         18. Event Type Visibility
         19. Icon Type Visibility
         20. Source Visibility
         21. Node Visibility
         22. Relationship ID
         23. Parent ID
         24. Child ID
         25. Label
         26. Associate parent and a child
      2. Can:
         1. Make a relationship between a parent and a child node.
         2. Allow user to select visibility settings of a node
            1. Node Id Visibility
            2. Node Name Visibility
            3. Node Timestamp Visibility
            4. Node Description Visibility
            5. Log Entry Reference Visibility
            6. Log Creator Visibility
            7. Event Type Visibility
            8. Icon Type Visibility
            9. Source Visibility
            10. Node Visibility
         3. Display node information
   2. Collaborators
      1. Receives information from Log Entry.
      2. Gets data from Icon.
7. Icon
   1. Responsibilities:
      1. Knows:
         1. Icon Name
         2. File Path
      2. Can:
         1. Stores the attributes it knows.
   2. Collaborators:
      1. Is based on the Node log creator.
8. GraphAndTable
   1. Responsibilities:
      1. Knows:
         1. Export Format
         2. Orientation
         3. Interval Units
         4. Interval
         5. Position of Nodes
         6. Position of Relationships
         7. At least one node
         8. Knows the size of the current graph/table
      2. Can:
         1. Can add new nodes.
            1. Adds a new row to the node table.
            2. Adds a new node to the nodes configuration in the graph.
         2. Can add relationship to nodes.
            1. Adds a new row in the relationship table.
            2. Adds a new relationship to the nodes configuration in the graph.
         3. Can delete relationships.
            1. The row in the relationship table shall be removed.
            2. The relationship in the nodes configuration in the graph shall be removed.
         4. Can display an error when the user attempts to delete a relationship when one is not selected.
         5. Can delete a node.
            1. The selected node in the table shall be removed.
            2. The selected node in the nodes configuration in the graph shall be removed.
         6. A display error is shown when the user attempts to delete a node when non is selected.
         7. When filtering is complete,
            1. The node table shall display nodes that meet the criteria.
            2. The relationship table shall display relationships that meet the criteria.
            3. The graph shall display nodes that meet the criteria.
         8. When the user selects to edit node the user will be able edit node contents
         9. Export graph in selected format
         10. Undo any changes to graph since last commit
         11. Commit any changes made to graph and save it
             1. Change should be saved in temporary storage
             2. Change should be logged in change list
         12. Change icon type of node
         13. Do “Add Icon” operation
         14. Do “Delete Icon” operation
         15. Allow nodes to be repositioned in graph
         16. Display nodes in graphical view
         17. Display nodes in table view
   2. Collaborators:
      1. Table gets data from Nodes.
      2. Graph gets data from Nodes.