CRC

**Nouns Phrases:**

Log entries

Log files

Nodes

Vectors

Graph

User

Images

Audio

Icon

Repository

Relationships

Change

Event Configuration

Directory Configuration

Vector Configuration

Log File Configuration

Filter Configuration

Log Entry Configuration

Export Configuration

Change Configuration

Vector DB Configuration

Icon Configuration

Graph Builder Configuration

Configuration

Team Configuration

Splunk

Optical Character Recognition (OCR)

Extract Transform Load (ETL)

Transcriber

Analyst

Lead

Enforcement action report

Significant log entry

root directory structure error

Wildcard searching

Logical searching

Vector DB

Filtering

Timestamp

Artifacts

Red team

Blue team

White team

Timeline

Node table

Log File Table

Log Entry Table

Vector DB Table

Relationship Table

CheckBox

Upward/Downward arrow

Label

Button

Dropdown Box

Text Field

Relationship ID

Event

Root Directory

Red Team Folder

Blue team Folder

White Team Folder

Error Message

Host

Log Creator

Parent ID

Child ID

Machine

Video

Record

Notification

**Choosing one word for a concept:**

1. Image File: image
2. Media File: Audio and Video
3. Searching:
4. Node Relationship: Relationship
5. Vector Timeline: Timeline
6. Vector DB: Vector DB and Repository
7. Vector: Vector and Record
8. Commit: Change

**Eliminate Things Outside of the System:**

1. Splunk
2. Machine

**Model Physical Objects:**

1. User
2. Analyst
3. Lead

**Model Conceptual Entities:**

1. Repository
2. Vector
3. Event
4. Host
5. Artifact

**Attributes:**

1. Timestamp
2. Notification
3. Error Message
4. Log Creator
5. Parent ID
6. Child ID
7. Relationship ID
8. White Team
9. Red Team
10. Blue Team
11. Text Field
12. CheckBox
13. Upward/Downward arrow
14. Label
15. Button
16. Dropdown Box
17. Icon
18. Root Directory
19. Red Team Folder
20. Blue team Folder
21. White Team Folder
22. Commit
23. Significant log entry
24. Enforcement Action Report

**Interfaces:**

1. Optical Character Recognition (OCR)
2. Extract Transform Load (ETL)
3. Transcriber

**CRC Card:**

1. Graph
   1. Responsibilities
      1. Creation of a visual graph and its visual elements (e.g., Nodes)
   2. Collaborations
      1. Node: Displaying nodes into the graph.
      2. Node Relationship: Display nodes relationship into the graph
      3. Timeline: Displays the Timeline into the graph
2. Graph Service
   1. Responsibilities
      1. Display visual elements into the corresponding graph.
   2. Collaboration
      1. Intake Nodes to display in the corresponding graph.
      2. Handle the creation of the relationship between two nodes.
      3. Handle the arrangements of nodes in correlation to the settings of the timeline that was created.
3. Access Control Service
   1. Responsibilities
      1. Grant and reject to actions of a user depending on their access control
   2. Collaborations
      1. Grand and reject the actions of an Analyst or Lead, depending on their access control level.
4. Analyst
   1. Superclass
      1. User
   2. Responsibilities
      1. Allow all the functionalities of the system except for the ‘*verify sync*’ function.
5. Lead
   1. Superclass
      1. User
   2. Responsibilities
      1. Allow the user to perform all functionalities of the system
6. Log Entry
   1. Responsibilities
      1. Represent the information a log entry contains in a system; this includes the flag that indicated of a log entry is *significant.*
   2. Collaboration
      1. ETL: The ETL is going to ingest log files and populate a log entry with the corresponding data.
      2. OCR: The OCR is going to populate log entry with captured data.
      3. Transcriber: The transcriber is going to populate log entry with captured data.
7. Node
   1. Responsibilities
      1. It contains the information of a visual representation of a *significant* log entry.
   2. Collaboration
      1. Graph: Graph displays a set of Nodes into the graph.
8. Vector
   1. Responsibilities
      1. It groups a set of *significant* log entries.
   2. Collaborations
      1. Log Entry: A vector comprises at least one significant log entry.
      2. Graph: Once a log entry is added to the Vector, the vector adds a Node representing the log entry to the graph.
9. Timeline
   1. Responsibilities
      1. Holds the general information about the time range of the nodes in the graph.
   2. Collaborations
      1. Graph: The graph is going to display the timeline in a given axis.
10. Log File
    1. Responsibilities
       1. Represents the actual log file the system is ingesting, furthermore, it contains the metadata of the file (last modification, absolute path, etc).
    2. Collaboration
       1. ETL: Log File is going to be transformed into a set of log entries.
11. Media File
    1. Superclass
       1. Log File
    2. Responsibilities
       1. Represents the audio data of a log file.
    3. Collaborations
       1. Transcriber: Going to transform the audio data into text.
12. Image File
    1. Superclass
       1. Log File
    2. Responsibilities
       1. Represents the image data of a log file.
    3. Collaborations
       1. OCR: Going to transform the image data into text.
13. Relationship
    1. Responsibilities
       1. Represents the relationship between two nodes, furthermore, it contains additional data, like Icon, text, arrow type, etc.
    2. Collaborations
       1. Graph: Displaying the visual arrow that dictates the relationship between the two nodes.
       2. Node: Signifies the relationship between two nodes.
14. Configuration
    1. Subclasses
       1. Event Configuration
       2. Directory Configuration
       3. Vector Configuration
       4. Log File Configuration
       5. Filter Configuration
       6. Log Entry Configuration
       7. Export Configuration
       8. Change Configuration
       9. Vector DB Configuration
       10. Icon Configuration
       11. Graph Builder Configuration
       12. Team Configuration
    2. Responsability
       1. Represents and assigns the different configuration values to a corresponding artifact.
    3. Collaboration
       1. Defines the configuration values or settings for a log entry, log file, vector, event, graph, filter, event, and change.
15. Search
    1. Subclasses
       1. Logical Search
       2. Wildcard Search
    2. Responsibility
       1. Given a set of data, being able to search through the data given a rule, for example, logical searching or wildcard searching.
    3. Collaboration
       1. Collaborate with the Table to perform different searches operating on a given set of data.
16. Table
    1. Subclasses
       1. Node table
       2. Log File Table
       3. Log Entry Table
       4. Vector DB Table
       5. Relationship Table
    2. Responsibility
       1. Dynamically display different types of data given to it; with the ability to support the integration of other classes that extend the functionalities (e.g., Search and Filter).
    3. Collaboration
       1. Collaborate with the various types of data that are going to be displayed in a tabular format. Types of data include Log Files, Log Entries, Vectors, Relationships, and Nodes.
       2. Classes that integrate to the table in a visual format to extend functionality; classes include the Search and Filter class.
17. Filter
    1. Responsibility
       1. Given a set of data filters based on predefined rules the data, only returning the data that satisfied the rule.
    2. Collaboration
       1. The Filter class collaborates with classes that represent data, for example, filtering through a set of log entries or log files. Classes that are able to be filtered and collaborate with the filter class are Log Files, Log Entries, Vectors, Relationships, and Nodes.
18. Vector DB
    1. Responsibility
       1. Responsible for keeping track of the changes performed to the *host’s* Vectors, furthermore, manage the incoming *pull and pull* request from users.
    2. Collaboration
       1. Collaborate with User’s subclasses to handle requests (pull and push requests).
19. Directory Structure Error
    1. Superclass
       1. Runtime Exception
    2. Responsibility
       1. Going to notify when the root directory fails to match the folder names specified in the event configuration.