**Class, Responsibility and Collaborator**

A Class Responsibility Collaborator (CRC) model is a collection of standard index cards that have been divided into four sections. A class represents a collection of similar objects, description is just a brief explanation of what the class does, a responsibility is something that a class knows or contains, and a collaborator is another class that a class interacts with to fulfill its responsibilities. Below we have used the CRC method to find classes for the PICK system.

List of Nouns:

* Log Entry
* ~~Significant Log Entry~~
* Analyst
* Lead
* ~~Repository~~
* ~~User’s Local Repository~~
* Event Configuration
* Log File
* Enforcement Action Report
* Vector
* Node
* ~~Icon~~
* Graph
* ~~Team~~
* ~~IP Address~~
* ~~Directory~~
* ~~White Team~~
* ~~Red Team~~
* ~~Blue Team~~
* Vector DB

List of Verbs:

* Generate Graph
* Create new nodes
* Correlate Activity to response
* Create Vector
* Establish Relationship between log entries and vectors
* Ingest Log
* Create and maintain vectors and graphs
* Approve or reject graphs
* Filter
* Push vector db: (send recent commit history)
* Pull vector db: (grab changes from lead)
* Data cleansing
* Data validation
* Data ingestion
* Structural check
* Generate enforcement action report
* Search

CRC CARDS

|  |  |  |  |
| --- | --- | --- | --- |
| Classes | Description | Responsibilities | Collaborators |
| Log Entry | Represents data of a log file after being cleansed, validated and ingested | 1. Knows start and end time of a single action from the event. 2. Knows its source document. 3. Knows a description of its activity. | Vector(2) |
| Node | Represents a significant log entry in the Graph | 1. Visually represents an event on the graph. | Graph(1)  Log Entry |
| Graph | Contains the visual representation of nodes and their relationships | 1. Visually represent events as nodes 2. Visually represent time between events | Node(1)  Vector(2) |
| Vector | Association of significant log entries | 1. Represents the correlation and association of log entries. | Log entry(1) |
| Event configuration | Defines the name of the attack, start time, end time, what analyst is the lead, and where to search for the Root directory containing Red, White, and Blue Teams Folder. | 1. Knows the name of the Event. 2. Knows the start and end time for the event. 3. Knows the location of the root directory. 4. Knows the locations of the team folders. 5. Sets the rules for validation. 6. Knows the amount of connections allowed to the host. 7. Knows who the lead analyst is the event. 8. Knows the lead Analyst’s IP address. | Lead(5)  Graph(2) |
| Log File | Contain the activities that occurred for a team during an attack or response to an attack event | 1. Knows activities occurring during a certain time frame. 2. Knows the activities that occurred in a response to attack. |  |
| Analyst/Client | Primary user, can edit events on vectors, create new log entries and nodes, and export them | 1. Can corollate events to a vector 2. Can push vector changes to vector data base 3. Can pull vector data from the vector data base | Vector (1) |
| Lead/Server | Oversees and controls changes made to the vector data base. | 1. Can approve or deny changes made to vectors | Analyst (1) |
| Enforcement Action Report | Describes why a log file failed to be ingested | 1. Knows the status of a log from being validated, ingested. 2. Displays error message on failure to validate, ingest | Log File (1,2) |
| Vector DB Manager | Responsible for all actions made to the vector data base. | 1. Allows for analysts to pull current set of vectors 2. Allows analysts to push new/updated vectors 3. Allows Lead to sync Vector DB. | Vectors(1)  Lead(1) |