TeamWork

Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK) Software CRC Document

Version 2.0

03/02/2020

Document Control

Approval

The Guidance Team and the customer shall approve this document.

Document Change Control

Initial Release:	1.0
Current Release:	2.0
Indicator of Last Page in Document:	&
Date of Last Review:	03/02/2020
Date of Next Review:	03/02/2020
Target Date for Next Update:	03/02/2020

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members:
Dr. Gates
Dr. Salamah
Dr. Roach
Elsa Tai Ramirez
Peter Hanson

Customer:
Dr. Oscar Perez
Vincent Fonseca
Herandy Denisse Vazquez
Baltazar Santaella
Florencia Larsen
Erick De Nava

Software Team Members:
Charlie Juarez
Miriam Juarez
Angelica Marquez
Andrew Munoz
Aaron Rodriguez

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
1.0	02/28/2020	Miriam Juarez	Section 1
1.1	02/28/2020	Charlie Juarez	Section 1
1.2	02/28/2020	Andy Munoz	Section 1
1.3	02/28/2020	Aaron Rodriguez	Section 1
1.4	02/28/2020	Angelica Marquez	Section 1
2.0	03/02/2020	Aaron Rodriguez	Formatting, Check

TABLE OF CONTENTS

1. Classes, Responsibilities, & Collaborations

1.1. Log File

- Description: A file of any type (i.e. csv, jpeg, pdf, etc…) that has been ingested by the system.
- Responsibilities
  - R.1-1 Knows its own file type.
  - R.1-2 Know ingestion errors (if any exist).
  - R.1-3 Know all its own log content.

Responsibilities	Responsibilities description	Collaborations
R.1-1	Knows its own file type	R.2-1
R.1-2	Know ingestion errors (if any exist)	
R.1-3	Know all its own log content	

1.2. Log Entry

- Description: Normalized data recovered from log files.
- Responsibilities
  - R.2-1 Know the attributes of Log Entry Number.
  - R.2-2 Know Log Entry Timestamp.
  - R.2-3 Know Log Entry Content.
  - R.2-4 Know Host, and Source.

Responsibilities	Responsibilities description	Collaborations
R.2-1	Know the attributes of Log Entry Number	R.1-3
R.2-2	Know Log Entry Timestamp	
R.2-3	Know Log Entry Content	
R.2-4	Know Host, and Source	

1.3. Event Configuration

- Description: Configuration for a project that determines the file paths and time restraints to place on log files to be ingested.
- Responsibilities:
  - R.3-1 Know the root path of log files, file path of red team log files, file path of blue team log files, file path of white team log files.
  - R.3-2 Know the time restraints on the log files.

Responsibilities	Responsibilities description	Collaborations
R.3-1	Know the root path of log files, file path of red team log files, file path of blue team log files, file path of white team log files.	R.1-3
R.3-2	Know the time restraints on the log files.	

1.4. Vector

- Description: Series of activities or steps that are necessary to achieve an object.
- Responsibilities
  - R.4-1 Know vector Name.
  - R.4-2 Know vector Description.
  - R.4-3 Vector Configuration has Add Vector, Delete vector, Edit vector, and a vector table.

Responsibilities	Responsibilities description	Collaborations

R.4-1	Know vector Name.	R.2-1
R.4-2	Know vector Description	
R.4-3	Vector Configuration has Add Vector, Delete vector, Edit vector, and a vector table	

1.5. Graph

- Description: A visual representation of a vector.
- Responsibility
    - R.5-1 Knows attributes of Orientation, Export Format, Interval Units, Interval, Position of Nodes, and Position of Relationships.
    - R.5-2 A Graph contains at least one node.

Responsibilities	Responsibilities description	Collaborations
R.5-1	Knows attributes of Orientation, Export Format, Interval Units, Interval, Position of Nodes, and Position of Relationships	R.4-2 R.6-1
R.5-2	Graph contains at least one node	R.6-2

1.6. Node

- Description: A visual representation of a significant event.
- Responsibilities:
    - R.6-1 Knows attributes of Node ID, Node Name, Node Timestamp, Node Description, Log Entry Reference, Log Creator, Event Type, Icon Type, Source, Node Visibility.
    - R.6-2 A Node is part of at least one graph.
    - R.6-3 Knows information about its relationships.

Responsibilities	Responsibilities description	Collaborations
R.6-1	Knows attributes of Node ID, Node Name, Node Timestamp, Node Description, Log Entry Reference (2), Log Creator, Event Type, Icon Type, Source, Node Visibility	R.9-2 R.9-1
R.6-2	A Node is part of at least one graph (5)	
R.6-3	Knows information about its relationships	

1.7. Filter

- Description: Used to display log entries that match the filter criteria.
- Responsibilities
    - R.7-1 Narrows down log entry search results to those that match the filter criteria
    - R.7-2 Has access to log entry data to match its filter criteria

Responsibilities	Responsibilities description	Collaborations
R.7-1	Narrows down log entry search results to those that match the filter criteria	R.2-1 … R.2-4
R.7-2	Has access to log entry data to match its filter criteria	

1.8. Enforcement Action Report

- Description: Contains error report information.
- Responsibility
    - R.8-1 Knows the attributes of Line Number and Error Message.
    - R.8-2 Has access to log file (1) data to acquire Line Number error information.

Responsibilities	Responsibilities description	Collaborations
R.8-1	Knows the attributes of Line Number and Error Message.	R.1-2

R.8-2	Has access to log file (1) data to acquire Line Number error information.	

1.9. Relationship

- Description: Establishes the association between parent and child node.
- Responsibilities
    - R.9-1 Knows attributes of relationship ID, Parent ID, Child ID, and Label
    - R.9-2 Has access to a parent node and a child node
    - R.9-3 Has a describing label of the association

Responsibilities	Responsibilities description	Collaborations
R.9-1	Knows attributes of relationship ID, Parent ID, Child ID, and Label.	R.6-1
R.9-2	Has access to a parent node (6) and a child node. (6)	
R.9-3	Has a describing label of the association.	

1.10. Main

- Description: Window in charge of handling transition to the project workspace
- Responsibilities:
    - R.10-1 Handle transitions to other windows

Responsibilities	Responsibilities description	Collaborations
R.10-1	Handle transitions to other windows	Handle transition to ProjectConfigWindow. Handle transition to NavigatorWindow.

1.11. ProjectConfigWindow

- Description: Window in charge of handling transition to the project workspace
- Superclass: main
- Responsibilities:
    - R.11-1 Retrieve directory path of log files
    - R.11-2 Handle event time range for the project.
    - R.11-3 Handle event name and description for the project.
    - R.11-4 Handle transition to ValidationIngestionWindow.

Responsibilities	Responsibilities description	Collaborations
R.11-1	Retrieve directory path of log files	Retrieve directory data from DirDialog. Send directory data to ValidationIngestionWindow. Send event date information to ValidationIngestionWindow
R.11-2	Handle event time range for the project	
R.11-3	Handle event name and description for the project	
R.11-4	Handle transition to ValidationIngestionWindow	

1.12. DirDialog

- Description: Window in charge of handling directory path
- Superclass: ProjectConfigWindow
- Responsibilities:
    - R.12-1 Retrieve directory path of log files

Responsibilities	Responsibilities description	Collaborations

R.12-1	Retrieve directory path of log files	Send directory path to ProjectConfigWindow.

1.13. ValidationIngestionWindow

- Description: Window in charge of handling the validation and ingestion process
- Superclass: ProjectConfigWindow
- Responsibilities:
  - R.13-1 Validate log file data
  - R.13-2 Ingest log file data
  - R.13-3 Handle log entries
  - R.13-4 Handle transition to NavigatorWindow

Responsibilities	Responsibilities description	Collaborations
R.13-1	Validate log file data	Send log file data to Splunk R.1-2
R.13-2	Ingest log file data	
R.13-3	Handle log entries	
R.13-4	Handle transition to NavigatorWindow	

1.14. Splunk

- Description: External software tool used in the creation of log entries.
- Superclass: ValidationIngestionWindow
- Responsibilities:
  - R.14-1 Transform log file data into log entries.
  - R.14-2 Archive log entries into a local database.

Responsibilities	Responsibilities description	Collaborations
R.14-1	Transform log file data into log entries.	Use MongoDB as the local database R.1-3
R.14-2	Archive log entries into a local database	

1.15. MongoDB

- Description: Window in charge of handling directory path
- Superclass: NavigatorWindow
- Responsibilities:
  - R.15-1 Store data from Splunk
  - R.15-2 Handle data management being imposed by NavigatorWindow

Responsibilities	Responsibilities description	Collaborations
R.15-1	Store data from Splunk	R.14-1 Work with NavigatorWidow to exchange data
R.15-2	Handle data management being imposed by NavigatorWindow	

1.16. NavigatorWindow

- Description: Window in charge of log entry handling.
- Superclass: ValidationIngestionWindow
- Responsibilities:

- R.16-1 Sort through log entry data.
- R.16-2 Prepare data changes for MongoDB.
- R.16-3 Create Vectors.

Responsibilities	Responsibilities description	Collaborations
R.16-1	Sort through log entry data.	Work with GraphTableWindow to exchange data. Send data changes to MongoDB. R.4-3 R.7-1
R.16-2	Prepare data changes for MongoDB.	
R.16-3	Create Vectors.	

1.17. GraphTableWindow

- Description: Window in charge of graphing log entry in vector format
- Superclass: NavigatorWindow
- Responsibilities:
  - R.17-1 Create vectors.
  - R.17-2 Show graphical representation of vectors.
  - R.17-3 Show table representation of vectors.
  - R.17-4 Edit graphical representation of vectors.
  - R.17-5 Edit table representation of vectors.
  - R.17-6 Create relationships among nodes.
  - R.17-7 Create nodes.

Responsibilities	Responsibilities description	Collaborations
R.17-1	Create vectors.	R.14-1 R.7-1 Work with NavigatorWidow to exchange data Send data changes to MongoDB.
R.17-2	Show graphical representation of vectors.	
R.17-3	Show table representation of vectors.	
R.17-4	Edit graphical representation of vectors.	
R.17-5	Edit table representation of vectors.	
R.17-6	Create relationships among nodes.	
R.17-7	Create nodes.	

&