<Enter team name here>

Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK) Software Requirements Specification

Version 1.7

1/21/2020

Document Control

Approval

The Guidance Team and the customers shall approve this document.

Document Change Control

Initial Release:	0.1
Current Release:	1.5
Indicator of Last Page in Document:	&
Date of Last Review:	01/29/2020
Date of Next Review:	02/07/2020
Target Date for Next Update:	02/10/2020

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

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

Software Team Members:
Team 1
Team 2
Team 3
Team 4
Team 5
Team 6
Team 7
Team 8
Team 9
Team 10
Team 11
Team 12
Team 13
Team 14
Team 15

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
0.1	01/15/2020	Elsa Tai Ramirez	Created a draft document
1.0	01/25/2020	Elsa Tai Ramirez	Completed the interface, real world object, and stimulus requirements.
1.5	1/29/2020	S. Roach	Minor Edits and actor descriptions
1.7	1/30/2020	S. Roach	Added use case descriptions and definitions, per E. Tai Ramirez

Table of Contents

1. Introduction

1.1. Purpose and Intended Audience

The purpose of the Software Requirements Specification (SRS) is to give the customer a clear and precise description of the functionality of the Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK). The SRS divides the system requirements into two parts, behavioral and non-behavioral requirements. The behavioral requirements describe the interaction between the system and its environment. Non-behavioral requirements relate to the definition of the attributes of the product as it performs its functions. This includes performance requirements of the product. The intended audience of the SRS is Dr. Oscar Perez, Mr. Vincent Fonseca, Ms. Herandy Vazquez, Mr. Baltazar Santaella, Ms. Florencia Larsen, and the Software Engineering teams. This document serves as an agreement between both parties regarding the product to be developed.

1.2. Scope of Product

The Lethality, Survivability, and HSI Directorate (LSH) recognizes the complexity and the time it takes to analyze the applicable logs, observation notes, and other artifacts gathered from an adversarial assessment from the red, blue, and white teams and generate a report that presents the events that took place during the adversarial assessment. They want a system that would aid their analysts in correlating red team's activities to blue team's responses and represent the events that took place during an adversarial assessment graphically.

The University of Texas at El Paso (UTEP) and LSH are collaborating to develop Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK) that will provide the ability to correlate red team's activities to blue team's responses and graphically represent the events that took place during an adversarial assessment.

1.3. Definitions, Acronyms, and Abbreviations

1.3.1. Definitions

The definitions in this section are given in the context of the product being developed. This intention is to assist the user in their understanding of the document.

Table 1: Definition of terms used in the report

TERM	DEFINITION
Actor	A representation in the use case diagram denoting external entities that interact with a system being modeled, e.g., the testbed management system.
Extend Relationship	Denotes insertion of optional behavior of another use case into the primary use case.
Generalization Relationship	Denotes a relationship between a general use case and a specific use case.
Include Relationship	Denotes the inclusion of behavior of another use case into the primary use case.
Use Case	A modeling technique that presents the basic functionality of a system and the actors that interact with each function.
Data Cleansing	Data cleansing is the removal of unwanted characters from uncleansed TMUX log file; removal of blank rows from uncleansed excel log file; and removal of blank lines from uncleansed log file.
Data Validation	Data validation is the process of inspecting data in the cleansed log files based on predefined data validation rules.

Log Entry	Splunk takes the validated log files and convert them into normalized data. The normalized data are called log entries. Users of the system can filter and edit log entries.
Significant Log Entry	A log entry selected by the user and associated with a vector. The attributes are the same as for a log entry. The system stores significant log entries. Splunk stores log entries in the normalized data files.
Timestamp	Denotes time in hours:minutes, date in month:date:year, and section in am/pm.
Text Label	Denotes a component that displays a single line of read-only, non-selectable text [2].
Text Field	Denotes a component that implements a single line of text [2].
Text Area	Denotes a component that displays multiple lines of text.
Significant log entry	Denotes a log entry that is associated to at least one vector.

1.3.2. Acronyms

This section lists the acronyms used in this document and their associated definitions.

Table 2: Acronyms

TERM	DEFINITION
SRS	Software Requirements Specification
UTEP	The University of Texas at El Paso
PICK	Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System
LSH	Lethality, Survivability, and HSI Directorate
PMR	Prevent, Mitigate, and Recover
IP	Internet Address
AA	Adversarial Assessment

1.3.3. Abbreviations

This section provides a list of used abbreviations and their associated definitions.

Table 3: Abbreviations

TERM	DEFINITION
e.g.	For example
i.e.	That is
TBD	To be determined

1.4. Overview

The SRS is divided into three major sections: Introduction (Section 1), General Description (Section 2), and Specific Requirements (Section 3).

Section 1 includes five subsections. Section 1.1 provides the purpose and intended audience of the document. Section 1.2 describes the scope of the product. Section 1.3 provides the definitions, acronyms and abbreviations. Section 1.4 provides the organization of the document. Section 1.5 lists the references used in this document.

Section 2 includes five subsections. Section 2.1 contains a description of the product, its overall structure, and its functionality. Section 2.2 summarizes the main features of the system. Section 2.3 identifies each type of users of the system. This is accomplished through a summary of actors and use-cases. Section 2.4 states existing general constraints. Section 2.5 gives the assumptions and dependencies of the system.

Section 3 includes four major subsections. Section 3.1 contains requirements that are related to the external interface. Section 3.2 contains the functional requirements that are organized in the following categories: same class of user, related real-world objects, stimulus, related features, and limits and default settings. Section 3.3 contains non-behavioral requirements.

1.5. References

[1] O. Perez et al, Requirements Definition Document, Lethality, Survivability and HSI Directorate, 2019.
[2] "Components and Containers in AWT". Internet:
https://www.cs.utexas.edu/~mitra/csSpring2009/cs313/lectures/GUIComponents.html, 2009 [Jan. 28, 2019]

2. General Description

2.1. Product Perspective

Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK) is an interactive system that facilitates correlations between red team's activities and blue team's responses and generates graphical representation of events that took place during an adversarial assessment.

2.2. Product Features

Figure 1 presents a level 1 use case diagram that provides an overview of the main functionalities provided by PICK and the interactions between actors and PICK. Figure 2 presents the notations used in a use case diagram. The actors, represented by stick figures, are external entities that interact with PICK. The use case, represented by ovals, elucidates the actors' interactions with PICK. Figure 3 presents a level 2 use case diagram that provides extensions of the functionalities, in particular the include, extend, and generalization interactions between the actors and the system. The include relationship denotes the inclusion of behavior of another use case into the primary use case. The extend relationship denotes insertion of optional behavior of another use case into the primary use case. The generalization relationship denotes a relationship between a general use case and a specific use case. These components are described next.

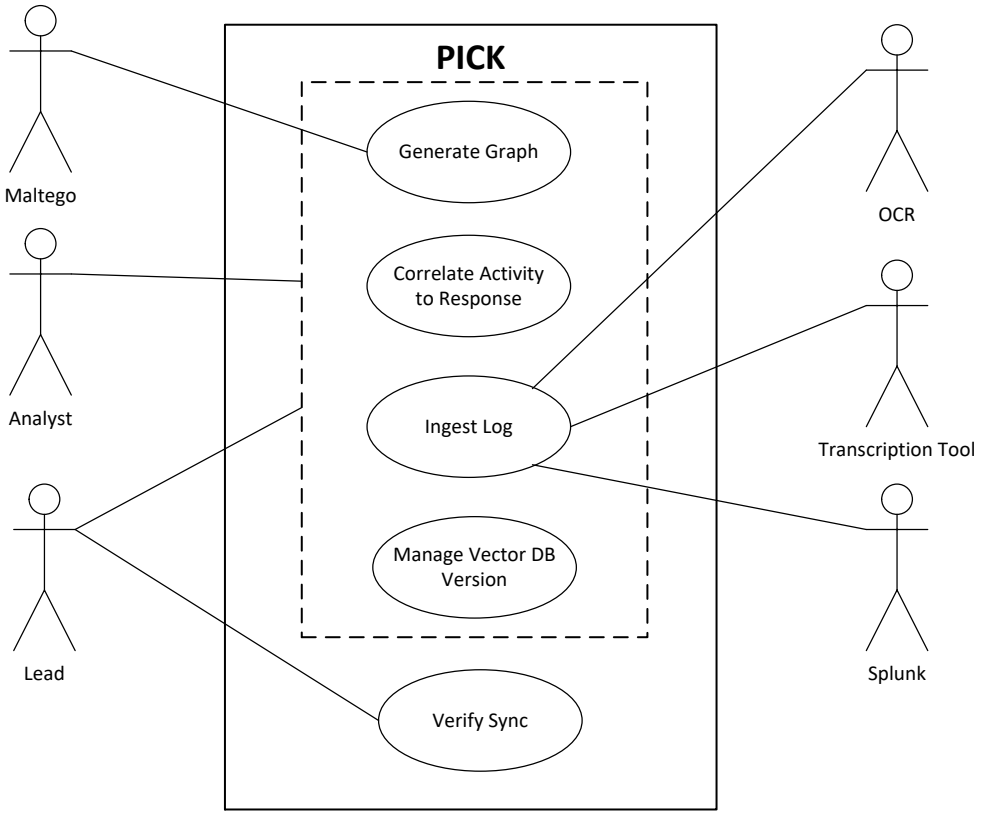

Figure 1: Level 1 Use Case Diagram

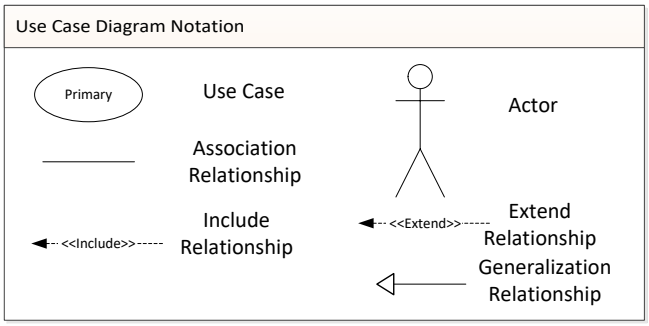

Figure 2: Use Case Diagram Notation

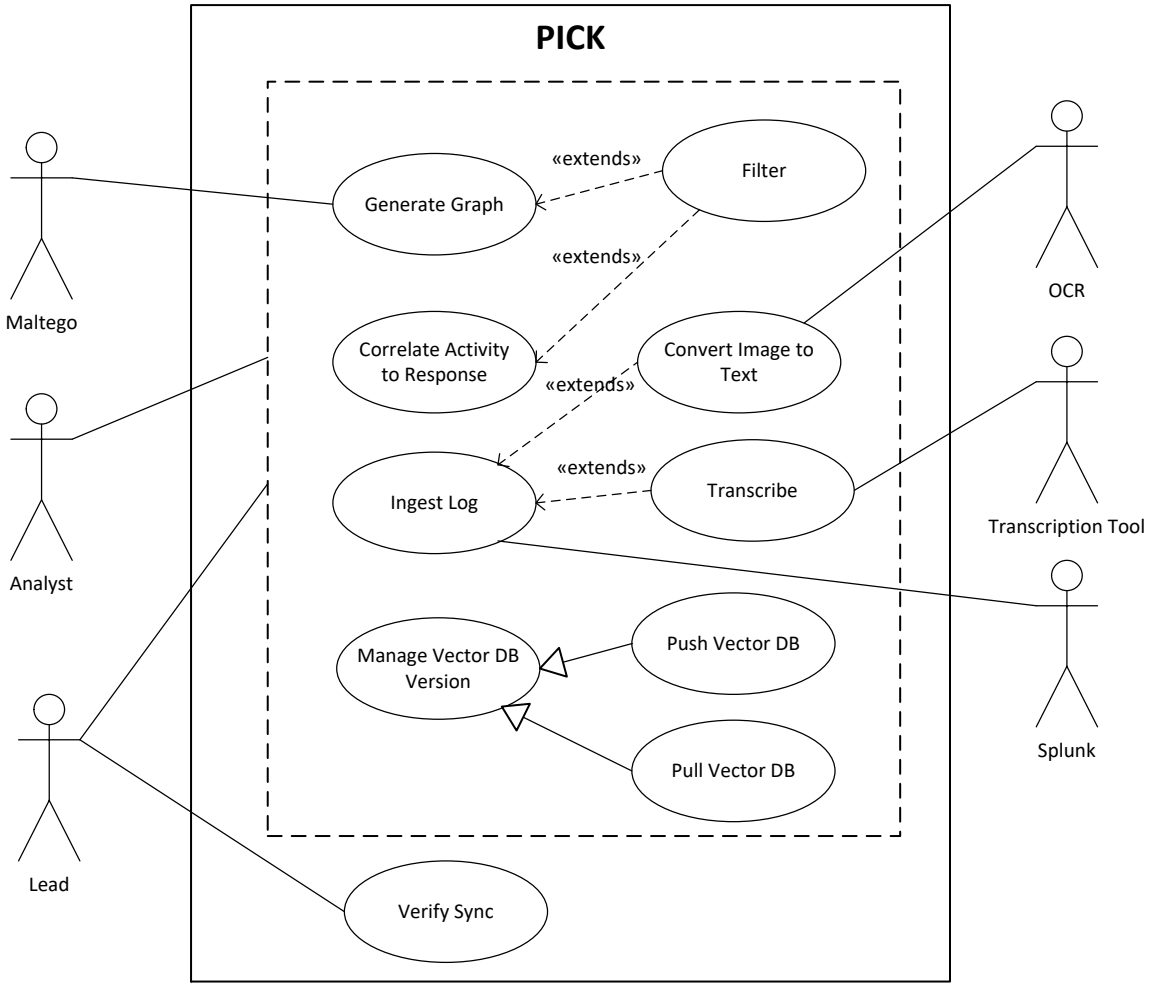

Figure 3: Level 2 Use Case Diagram

2.2.1. Actors Descriptions

PICK classifies the actors into the following groups:

- Analyst: The principal user of the system
- Lead: A user with all the privileges of an Analyst, but can also verify
- Maltego: A third party graphing tool
- OCR: An optical character recognition software tool (specific software not specified)
- Transcription Tool: A voice-to-text transcription software tool (specific software not specified)

- Splunk: A software tool for transforming log files into normalized log entries

2.2.2. Use Case Descriptions

PICK supports the following primary use cases:

- Generate Graph: Create a visual representation of a vector by allowing the user to establish relationships between nodes and create new nodes to capture activities that are not associated with significant log entries.
- Correlate Activity to Response: Create vector and establish relationship between log entries and vectors,
- Ingest Log: Convert log files to normalized data.
- Manage Vector DB Version: Create and maintain vectors and graphs.
- Verify Sync: Approve or reject graphs submitted by users.

PICK supports the following secondary use cases:

- Filter: Display log entries, nodes, or relationships that match the filter criteria.
- Convert Image to Text: Convert images of typed text and scanned document into machine-encoded text.
- Transcribe: Convert audio to text.
- Push Vector DB: Send recent commit history from the user's repository to lead's repository.
- Pull Vector DB: Grab changes from lead's repository into the user's local repository.

2.3. User Characteristics

The users of the system have a variety of computer usage skills and are immersed in the area of cybersecurity and network.

2.4. General Constraints

The general constraints on the development of PICK are as follows:

- The system will be completed by the end of Spring 2020.
- The system will be developed in Python3.
- Any software the system is interfacing with will need to be air-gap.

2.5. Assumptions and Dependencies

The assumptions and dependencies of PICK are as follows:

- The clients will provide the unwanted character removal script.

3. Specific Requirements

3.1. External Interface Requirements

This section contains the specification of requirements for interfaces among different components and their external capabilities.

3.1.1. User Interfaces

This section describes the characteristics of each interface of PICK. The interfaces listed below will be described in the following sections:

- Team Configuration
- 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
- Nodes Configuration in Tabular Format
- Nodes Configuration in Graphical Format
- Relationship Configuration

3.1.1.1. Team Configuration

[SRS 1] The team configuration shall have the following components:

a. A label labeled as “Team configuration”
b. A check box labeled as “Lead”
c. A text field labeled as “Lead IP address”
d. A label labeled as “No. of established connections to the lead’s IP address”
e. A label labeled with the number of connections to the lead’s IP address.
f. A button labeled as “Connect”.

3.1.1.2. Event Configuration

[SRS 2] The event configuration shall have the following components:

a. A label labeled as “Event configuration”
b. A text field labeled as “Event name”
c. A text field labeled as “Event description”
d. A text field labeled as “Event start timestamp”
e. A text field labeled as “Event end timestamp”.
f. A button labeled as “Save event”.

3.1.1.3. Directory Configuration

[SRS 3] The directory configuration shall have the following components:

a. A label labeled as “Directory configuration”
b. A text field labeled as “Root directory”

c. A text field labeled as “Red team folder”
d. A text field labeled as “Blue team folder”
e. A text field labeled as “White team folder”
f. A button labeled as “Start data ingestion”.

3.1.1.4. Vector Configuration

[SRS 4] The vector configuration shall have the following components:
a. A label labeled as “Vector configuration”
b. A vector table
c. A button labeled as “Add vector”
d. A button labeled as “Delete vector”
e. A button labeled as “Edit vector”.

[SRS 5] The vector table in the vector configuration shall include the following components:
a. A column of check boxes
b. A column of text fields with the column header labeled as “Vector name”
c. An upward/downward arrow within the column header labeled as “Vector name”
d. A column of text fields with the column header labeled as “Vector description”
e. An upward/downward arrow within the column header labeled as “Vector description”.

3.1.1.5. Log File Configuration

[SRS 6] The log file configuration shall have the following components:
a. A label labeled as “Log file configuration”
b. A log file table
c. An enforcement action report table.

[SRS 7] The log file table in the log file configuration shall include the following components:
a. A column of labels with the column header labeled as “File name”
b. An upward/downward arrow within the column header labeled as “File name”
c. A column of labels with the column header labeled as “Source”
d. An upward/downward arrow within the column header labeled as “Source”
e. A column of labels with the column header labeled as “Cleansing status”
f. An upward/downward arrow within the column header labeled as “Cleansing status”
g. A column of labels with the column header labeled as “Validation status”
h. An upward/downward arrow within the column header labeled as “Validation status”
i. A column of labels with the column header labeled as “Ingestion status”
j. An upward/downward arrow within the column header labeled as “Ingestion status”
k. A column of buttons with the column header labeled as “View enforcement action report”.

[SRS 8] The enforcement action report table in the log file configuration shall include the following components:
a. A label labeled as “File name:”
b. A label labeled with the name of the selected log file
c. A column of labels with the column header “Line number”
d. An upward/downward arrow within the column header labeled as “Line number”
e. A column of labels with the column header labeled as “Error message”
f. An upward/downward arrow within the column header labeled as “Error message”
g. A button labeled as “Validate”
h. A button labeled as “Cancel”.

3.1.1.6. Filter Configuration

[SRS 9] The filter configuration shall have the following components:
a. A label labeled as “Filter configuration”
b. A text field labeled as “Keyword search”

c. A label labeled as “Creator”
d. A check box labeled as “Red”
e. A check box labeled as “White”
f. A check box labeled as “Blue”
g. A label labeled as “Event type”
h. A check box labeled as “Red”
i. A check box labeled as “White”
j. A check box labeled as “Blue”
k. A text field labeled as “Start timestamp”
l. A text field labeled as “End timestamp”
m. A button labeled as “Apply Filter”.

3.1.1.7. Log Entry Configuration

[SRS 10] The log entry configuration shall have the following components:
a. Label labeled as “Log entry configuration”
b. A Log entry table.

[SRS 11] The log entry table in the log entry configuration shall include the following components:
a. A column of check boxes
b. A column of text fields with the column header labeled as “List number”
c. An upward/downward arrow within the column header labeled as “List number”
d. A column of text fields with the column header labeled as “Log entry timestamp”
e. An upward/downward arrow within the column header labeled as “Log entry timestamp”
f. A column of text fields with the column header labeled as “Log entry event (including Log entry content, host, source, sourcetype)”
g. An upward/downward arrow within the column header labeled as “Log entry event”
h. A column of dropdown boxes with the column header labeled as “Vector”.

3.1.1.8. Export Configuration

[SRS 12] The export configuration shall have the following components:
a. A dropdown box labeled as “Export format”
b. A button labeled as “Export”.

3.1.1.9. Change Configuration

[SRS 13] The change configuration shall have the following components:
a. A text area labeled as “Change list”
b. A button labeled as “Undo”
c. A button labeled as “Commit”.

3.1.1.10. Vector DB Configuration

[SRS 14] The vector DB configuration for analyst shall have the following components:
a. A label labeled as “Connection status to lead:”
b. A label labeled with the connection status
c. A label labeled as “Pulled vector DB table (Analyst)”
d. A pulled vector DB table
e. A button labeled as “Pull”
f. A label labeled as “Pushed vector DB table (Analyst)”
g. A pushed vector DB table
h. A button labeled as “Push”.

[SRS 15] The pulled vector DB table (analyst) in the vector DB configuration shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Vector”
c. An upward/downward arrow within the column header labeled as “Vector”
d. A column of text fields with the column header labeled as “Description”
e. An upward/downward arrow within the column header labeled as “Description”
f. A column of graphs with the column header labeled as “Graph”.

[SRS 16] The pushed vector DB table (analyst) in the vector DB configuration shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Vector”
c. An upward/downward arrow within the column header labeled as “Vector”
d. A column of text fields with the column header labeled as “Description”
e. An upward/downward arrow within the column header labeled as “Description”.
f. A column of graphs with the column header labeled as “Graph”.

[SRS 17] The vector DB configuration for lead shall have the following components:

a. A label labeled as “Approval sync:”
b. An approval vector DB sync table
c. A button labeled as “Commit”.

[SRS 18] The approval vector DB sync table in the vector DB configuration shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Source IP”
c. An upward/downward arrow within the column header labeled as “Source IP”
d. A column of text fields with the column header labeled as “Request timestamp”
e. An upward/downward arrow within the column header labeled as “Request timestamp”
f. A column of text fields with the column header labeled as “Vector”
g. An upward/downward arrow within the column header labeled as “Vector”
h. A column of text fields with the column header labeled as “Description”
i. An upward/downward arrow within the column header labeled as “Description”
j. A column of graphs with the column header labeled as “Graph”
k. A column of text fields with the column header labeled as “Change summary”
l. An upward/downward arrow within the column header labeled as “Change summary”
m. A column of dropdowns with the column header labeled as “Sync status”
n. An upward/downward arrow within the column header labeled as “Sync status”.

3.1.1.11. Icon Configuration

[SRS 19] The icon configuration shall have the following components:

a. A label labeled as “Icon configuration”
b. An icon table
c. A button labeled as “Add Icon”
d. A button labeled as “Delete Icon”
e. A button labeled as “Edit Icon”.

[SRS 20] The icon table in the icon configuration shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Icon name”
c. An upward/downward arrow within the column header labeled as “Icon name”
d. A column of text fields with the column header labeled as “Icon source”
e. An upward/downward arrow within the column header labeled as “Icon source”
f. A column of images with the column header labeled as “Image preview”
g. An upward/downward arrow within the column header labeled as “Image preview”

3.1.1.12. Graph Builder Configuration

[SRS 21] The graph builder configuration shall have the following components:
a. A dropdown box labeled as “Vector”
b. A label labeled as “Description:”
c. A label labeled with the description of the selected vector
d. A button labeled as “Add node”
e. A button labeled as “Add relationship”
f. A button labeled as “Delete node”
g. A button labeled as “Delete relationship
h. A button labeled as “Edit node”
i. A button labeled as “Edit relationship.

3.1.1.13. Nodes Configuration in Tabular Format

[SRS 22] The nodes configuration in tabular format shall have the following components:
a. A label labeled as “Nodes configuration in tabular format”
b. A node table.

[SRS 23] The node table in the nodes configuration in tabular format configuration shall include the following components:
a. A column of check boxes
b. A row of toggles with the row header labeled as “Node property visibility”
c. A column of labels with the column header labeled as “Node ID”
d. An upward/downward arrow within the column header labeled as “Node ID”
e. A column of text fields with the column header labeled as “Node name”
f. An upward/downward arrow within the column header labeled as “Node name”
g. A column of text fields with the column header labeled as “Node timestamp”
h. An upward/downward arrow within the column header labeled as “Node timestamp”
i. A column of text fields with the column header labeled as “Node description”
j. An upward/downward arrow within the column header labeled as “Node description”
k. A column of text fields with the column header labeled as “Log entry reference”
l. An upward/downward arrow within the column header labeled as “Log entry reference”
m. A column of dropdown boxes with the column header labeled as “Log creator”
n. An upward/downward arrow within the column header labeled as “Log creator”
o. A column of dropdown boxes with the column header labeled as “Event type”
p. An upward/downward arrow within the column header labeled as “Event type”
q. A column of dropdown boxes with the column header labeled as “Icon type”
r. An upward/downward arrow within the column header labeled as “Icon type”
s. A column of text fields with the column header labeled as “Source”
t. An upward/downward arrow within the column header labeled as “Source”
u. A column of toggles with the column header labeled as “Node visibility”
v. An upward/downward arrow within the column header labeled as “Node visibility”.

3.1.1.14. Nodes Configuration in Graphical Format

[SRS 24] The nodes configuration in graphical format shall have the following components:
a. A label labeled as “Nodes configuration in graphical format”
b. A dropdown box labeled as “Timeline orientation”

c. A dropdown box labeled as “Interval units”
d. A text field labeled as “Interval”
e. A timeline
f. A set of nodes with node properties
g. A set of relationships with their associated label
h. A button labeled as “Zoom in”
i. A button labeled as “Zoom out”.

[SRS 25] The system shall display the nodes configuration in tabular format and graphical format simultaneously.

3.1.1.15. Relationship Configuration

[SRS 26] The relationship configuration shall have the following components:
a. A label labeled as “relationship configuration”
b. A relationship table.

[SRS 27] The relationship table in the relationship configuration shall include the following components:
a. A column of check boxes
b. A column of labels with the column header labeled as “Relationship ID”
c. An upward/downward arrow within the column header labeled as “Relationship ID”
d. A column of text fields with the column header labeled as “Parent”
e. An upward/downward arrow within the column header labeled as “Parent”
f. A column of images with the column header labeled as “Child”
g. An upward/downward arrow within the column header labeled as “Child”
h. A column of images with the column header labeled as “Label”
i. An upward/downward arrow within the column header labeled as “Label”.

3.1.2. Hardware Interfaces

There are no hardware interface requirements specified at this time.

3.1.3. Software Interfaces

This section describes the characteristics of each interface between other application systems and the system.

[SRS 28] The system shall interface with Splunk to transform a log file into normalized log entries.

[SRS 29] The system shall interface with Maltego to create graphs with nodes and relationships between nodes.

[SRS 30] The system shall interface with a transcription software to transcribe audio file to text.

[SRS 31] The system shall interface with an optical character recognition software to perform conversion of images of typed text and scanned document into machine-encoded text.

3.1.4. Communications Interfaces

There are no communication interface requirements specified at this time.

3.2. Behavioral Requirements

This section describes the behavioral requirements of the system.

3.2.1. Same Class of User

This section describes requirements associated with a particular class of user.

[SRS 32] The system shall have two levels of access privileges: Analyst and Lead.

[SRS 33] A user who has Lead access privilege shall be able to perform all functionalities of the system.

[SRS 34] A user who has Analyst access privilege shall be able to perform all functionalities of the system except verify sync from analysts.

3.2.2. Related Real-world Objects

This section describes related real-world object requirements of the system.

3.2.2.1. Event Configuration

[SRS 35] The system shall store the attributes as defined in Table 4 for an event configuration.

Table 4: Event configuration

Attribute	Data Type	Values and Constraints	Description
Event Name	String	Required; Editable	Name of the AA event.
Event Description	String	Required; Editable	Description of the AA event.
Event Start Timestamp	Date Time	Required; Editable; Must be in Zulu Time; Format: HH:MM MM/DD/YY AM/PM	Start date and time of the AA event.
Event End Timestamp	Date Time	Required; Editable; Must be in Zulu Time; Format: HH:MM MM/DD/YY AM/PM	End date and time of the AA event.
Root Directory	String	Required; Not editable after structure validation	Path to where the log files are stored.
Red Team Folder	String	Required; Not editable after structure validation	Name of the folder where all the red team log files are stored.
White Team Folder	String	Required; Not editable after structure validation	Name of the folder where all the white team log files are stored.
Blue Team Folder	String	Required; Not editable after structure validation	Name of the folder where all the blue team log files are stored.
Lead	Boolean	Required; Editable; {Lead, Analyst}	Indictor of the host machine where the master vector DB is stored.
Lead's IP Address	String	Required; Editable	Identifier of the host machine where the master vector DB is stored.
Connection Established	Integer	Required; Not editable; Max value: 20	Number of established connections to the host machine.

3.2.2.2. Log File

[SRS 36] The system shall store the attributes as defined in Table 5 for a log file.

Table 5: Log File

Attribute	Data Type	Values and Constraints	Description
Log File Name	String	Required; Not editable	Name of the log file.
Cleansing Status	Boolean	Required; {Cleansed, Uncleansed}; Not editable	Indicator whether the unwanted characters, blank rows and lines are removed. Cleansed refers to the all unwanted characters, black rows and lines are removed. Uncleansed refers to the process of cleansing has not begun.
Validation Status	String	Required; {Validated, Not-validated, Invalid}; Not editable	Indicator whether the log file passes the data validation test. Validated refers to the log file passing all the data validation tests. Not-validated refers to the process of validation has not begun. Invalid refers to the log file fails in one or more data validation tests.
Ingestion Status	Boolean	Required; {Ingested, Not Ingested; Not editable	Indicator whether the log file has been converted into log entries. Ingested refers to Splunk successfully ingests the log file and turn it into log entries. Not ingested refers to the process of ingestion has not begun.
Acknowledgement Status	Boolean	Optional; {Accept, Reject}; Editable	Indicator whether the system should accept the log file as validated log file. Accept refers to confirmation from the analyst that the log file will be certified as validated log file

			regardless of the validation status. Reject refers to the analyst not certifying the log file as validated log file.

[SRS 37] The system shall store the cleansed log files in permanent storage.

[SRS 38] The system shall store significant log entries in permanent storage.

3.2.2.3. Enforcement Action Report

[SRS 39] The system shall store the attributes as defined in Table 6 for an enforcement action report.

Table 6: Enforcement Action Report

Attribute	Data Type	Values and Constraints	Description
Line Number	Integer	Required; Not editable	Location of where the error occurs in a log file.
Error Message	String	Required; Not editable	Explanation of why a specific line in the log file fails validation test.

3.2.2.4. Vector

[SRS 40] The system shall store the attributes as defined in Table 7 for a vector.

Table 7: Vector

Attribute	Data Type	Values and Constraints	Description
Vector Name	String	Required; Editable	Series of activities or steps an adversary executes or attempts to execute that are necessary to achieve an object.
Vector Description	String	Required; Editable	Description of the vector.

[SRS 41] A vector shall comprise of at least one significant log entry.

3.2.2.5. Significant Log Entry

[SRS 42] The system shall store the attributes as defined in Table 8 for a significant log entry.

Table 8: Log Entry

Attribute	Data Type	Values and Constraints	Description
Log Entry Number	Integer	Required	Unique identifier of a log entry.
Log Entry Timestamp	Data Time	Required; Editable; Must be in Zulu Time; Format: HH:MM MM/DD/YY AM/PM	Time and date of when the activity described by the log entry took place.
Log Entry Content	String	Required; Editable	Description of the activity.
Host	String	Required; Editable	IP address
Source	String	Required; Not Editable	Name and location of the log file from which a

			particular activity originates.
Source Type	String	Required; Not Editable	It refers to how Splunk software processes the incoming data stream into individual activities according to the nature of the data.

[SRS 43] A significant log entry shall be part of at least one vector.

3.2.2.6. Node

[SRS 44] The system shall store the attributes as defined in Table 9 for a node.

Table 9: Node

Attribute	Data Type	Values and Constraints	Description
Node ID	String	Required; Not editable	Unique identifier of a node.
Node Name	String	Required; Editable	Unique name of a node.
Node Timestamp	Date Time	Required; Editable; Must be in Zulu Time; Format: HH:MM MM/DD/YY AM/PM	Time and date of when the activity described by the significant log entry took place. Initially these are the same as for Significant Log Entry.
Node Description	String	Required; Editable; Initial value: Description of the log entry	Description of the activity. Initially these are the same as for Significant Log Entry.
Log Entry Reference	String	Optional; Editable	Link to the significant log entry.
Log Creator	String	Required; Editable; {White, blue, red}	Team who created the log.
Event Type	String	Required; Editable; {White, blue, red}	Team who executed the activity.
Icon Type	String	Required; Editable; Default: Circle	Path to an image used to reflect the nature of the activity.
Source	String	Optional; Editable	Name and location of the log file from which a particular activity originates.
Node Visibility	Boolean	Required; Editable	Indicator whether the node will be visible on a graph.

[SRS 45] A node shall be part of at least one graph.

[SRS 46] The system shall store the attributes as defined in Table 10 for the visibility of a node's attribute as defined in Table 10.

Table 10: Visibility of a Node's Attribute

Attribute	Data Type	Values and Constraints	Description
Node ID Visibility	Boolean	Required; Not editable; The visibility of Node ID is on by default; The impact of the node ID visibility affects all nodes in a graph.	
Node Name Visibility	Boolean	Required; Editable; {On, Off}; The impact of the node name visibility affects all nodes in a graph.	
Node Timestamp Visibility	Boolean	Required; Editable; {On, Off}; Initial value: On; The impact of the node timestamp visibility affects all nodes in a graph.	
Node Description Visibility	Boolean	Required; Editable; {On, Off}; Initial value: On; The impact of the node description visibility affects all nodes in a graph.	
Log Entry Reference Visibility	Boolean	Required; Editable; {On, Off}; The impact of the log entry reference visibility affects all nodes in a graph.	
Log Creator Visibility	Boolean	Required; Editable; {On, Off}; The impact of the log creator visibility affects all nodes in a graph.	
Event Type Visibility	Boolean	Required; Editable; {On, Off}; The impact of the event type visibility affects all nodes in a graph.	
Icon Type Visibility	Boolean	Required; Editable; {On, Off}; The impact of the icon type visibility affects all nodes in a graph.	
Source Visibility	Boolean	Required; Editable; {On, Off}; The impact of the source visibility affects all nodes in a graph.	
Node Visibility	Boolean	Required; Not editable; The visibility of node visibility is off.	

[SRS 47] The system shall store the attributes as defined in Table 11 for relationship.

Table 11: Relationship

Attribute	Data Type	Values and Constraints	Description
Relationship ID	String	Required; Not editable	Unique ID
Parent ID	String	Required; Editable; Parent node cannot be the same as the child node.	Source node of the relationship.

Child ID	String	Required; Editable; Child node cannot be the same as the parent node.	Destination node of the relationship.
Label	String	Required; Editable	Description of the relationship between the source and destination nodes.

[SRS 48] A relationship shall associate a parent and a child node.

3.2.2.7. Icon

[SRS 49] The system shall store the attributes as defined in Table 12 for icon.

Table 12: Icon

Attribute	Data Type	Values and Constraints	Description
Icon Name	String	Required; Editable	Name of the icon
File Path	String	Required; Editable;	Location of the file

3.2.2.8. Graph

[SRS 50] The system shall store the attributes as defined in Table 13 for graph.

Table 13: Graph

Attribute	Data Type	Values and Constraints	Description
Export Format	String	Required; Editable; {PNG, JPG}	
Orientation	Boolean	Required; {Horizontal, Vertical}	
Interval Units	String	Required; {Second, Minute, Hour, Day, Week}	
Interval	Integer	Required; Value has to be greater than 0.	
Position of Nodes	Set	Required; Editable; Initial Value: Chronological Order based on the node's timestamp.	
Position of Relationships	Set	Required; Editable; Initial Value: Null.	

[SRS 51] A graph shall comprise of at least one node.

3.2.3. Stimulus

This section describes the stimulus requirements of the PICK.

3.2.3.1. General

[SRS 52] When the user presses the "OK" button on the overlay, the system shall close the overlay.

[SRS 53] When the user presses the "X" button on the overlay, the system shall dismiss the overlay.

[SRS 54] When the user presses the "downward arrow" at the column header, the system shall display the content of the column in descending order.

[SRS 55] When the user presses the “upward arrow” at the column header, the system shall display the content of the column in ascending order.

3.2.3.2. Team

[SRS 56] When the user selects the “connect” operationand the following conditions are true, the system shall establish the connection to the lead’s machine:

a. Lead check box is unchecked
b. Lead’s IP address is not empty
c. The IP address of the local machine is not the same as the lead’s IP address.

[SRS 57] If the IP address of the local machine is the same as the lead’s IP address, the system shall display an error message.

[SRS 58] If the user selects the “connect” operationwithout providing the Lead’s IP address, the system shall display an error message.

[SRS 59] If the user selects the “connect” operationwith the lead check box selected, the system shall display an error message.

[SRS 60] If the number of established connections to the Lead’s IP exceeds 20 connections, the system shall display an error message.

3.2.3.3. Directory

[SRS 61] When the user selects the “start data ingestion” operation, the system shall perform the structure check.

[SRS 62] When the structural check operation is complete, the following properties pertaining of the root directory shall be true:

a. The root directory shall contain three folders.
b. 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.
c. The name of the root directory shall not be editable once the event is saved.

[SRS 63] If the root directory fails to contain three folders, the system shall generate a root directory structure error.

[SRS 64] If the folders contain in the root directory fails to match the folder names specified in the event configuration, the system shall generate a root directory structure error.

[SRS 65] When the structure check is complete, the system shall perform the data cleansing operation.

3.2.3.4. Log File

[SRS 66] When the data transformation operation of a log file is complete, the following properties of the log file shall be true:

a. The log file shall contain transcription of the audio clip with timestamps in one minute interval if the log file is of type “audio”.
b. The log file shall contain transcription of the audio clip from a video log file with timestamps in one minute interval if the log file is of type “video”.
c. The log file shall contain extracted text with the image if the log file is of type “image”.
d. The log file shall contain extracted text with the scanned image if the log file is of type “pdf”.

[SRS 67] When the data cleansing operation of a log file is complete, the following properties of the log file shall be true:

a. The log file shall contain no blank lines.

b. The log file shall contain no unwanted character if the log file is of type TMUX.
c. The log file shall contain no blank rows if the log file is of type CVS.
d. The log file shall be certified as cleansed log file.
e. The cleansed log file shall be saved.
f. The cleansing status of the log file shall be marked as “cleansed”.

[SRS 68] When the data cleansing operation of a log file is complete, the system shall perform the data validation operation.

[SRS 69] When the data validation operation is complete, the following properties of the log file shall be true:
a. The log file shall contain a timestamp per line.
b. The log file shall contain timestamps that are bounded by the start data, end date, start time, and end time specified in the event configuration.
c. If the log file is of type CVS and the originator of the log file is from the white team, the following addition properties of the log file shall be true:
d. The log file shall contain timestamps that are within the following range:
e. Lower limit of the range: (average of the start and end timestamps in the CSV file) minus 23 hours and 59 mins.
f. Upper limit of the range: (average of the start and end timestamps in the CSV file) plus 23 hours and 59 mins.
g. The log file shall be certified as validated log file.
h. The validation status of the log file shall be “pass”.

[SRS 70] If the data validation operation is incomplete, the system shall generate an enforcement action report and set the validation status of the log file to “fail”.

[SRS 71] When the verification action confirmation is received, the system shall certify the cleansed log file as validated log file.

[SRS 72] When the data validation operation is complete, the system shall perform the data ingestion operation.

[SRS 73] When the data ingestion operation is complete, the system shall set the ingestion status of a log file to “pass”.

[SRS 74] When the user selects the “view enforcement action report” operation, the system shall display the line numbers and error messages pertaining to the selected log file in the enforcement action table.

[SRS 75] When an ingested log file has been updated, the following shall be true:
a. The system shall treat the updated ingested log file as an uncleansed log file.
b. If the log file is ingested, the following properties of its log entries shall be true:
    i. A duplicate log entry shall be deleted.
    ii. An updated log entry shall be saved as a new log entry.
    iii. A new log entry shall be saved.

[SRS 76] If a folder in the root directory has sub folders, the system shall traverse through the sub folders and perform data cleansing operation on the log files that are in the sub folders.

[SRS 77] When a timestamp property of a previously saved event is changed, the impact of the change shall be restricted to the “not-validated” log files.

3.2.3.5. Search and Filter

[SRS 78] When a search operation is complete, the system shall return result that matches the searched keyword with the searched keyword highlighted in the search result.

[SRS 79] When the user is performed a search, the following search mechanism shall be supported:

a. Logical searching
b. Wildcard searching.

3.2.3.6. Vector

[SRS 80] When changes are made to a vector, the system shall auto save the changes to permanent storage.

[SRS 81] When the user presses on the “edit” button in the log entry table, the system shall enable the user to edit the selected log entry.

3.2.3.7. Vector DB

[SRS 82] When the connection between the lead and the user is established, the following properties of the vector database shall be true:

a. Differences between the corresponding records (vector and its associated graph) in the lead’s vector DB and the user’s vector DB shall be flagged.
b. Any record that exists in the lead’s vector DB and not in the user’s vector DB shall be visible to the user.

[SRS 83] When the user activates the “pull” operation, the system shall download the selected vector and its associated graph from the lead’s vector DB and add it to the user’s vector DB.

[SRS 84] When the user activates the “push” operation with a record selected, the system shall do the following:

a. The lead shall receive a push notification with the selected record.
b. The lead shall be able to view the selected record.
c. The selected record shall be stored in the lead’s vector DB if the lead approves the pushed record.

3.2.3.8. Graph

[SRS 85] At the completion of the “add node” operation, the following shall be true:

a. A new row shall be added to the node table.
b. A new node shall be added to the nodes configuration in graphical format section.

[SRS 86] At the completion of the “add relationship” operation, the following shall be true:

a. A new row shall be added to the relationship table.
b. A new relationship shall be added to the nodes configuration in graphical format section.

[SRS 87] At the completion of the “delete relationship” operationwith a relationship selected, the following shall be true:

a. The selected row in the relationship table shall be removed.
b. The corresponding relationship in the nodes configuration in graphical format section shall be removed.

[SRS 88] When the user attempts the “delete relationship” operationwithout selecting a relationship, the system shall generate an error.

[SRS 89] At the completion of the “delete node” operationwith a node selected, the following shall be true:

a. The selected node in the node table shall be removed.
b. The selected node in the nodes configuration in graphical format section shall be removed.

[SRS 90] When the user attemptsthe “delete node” operationwithout selected a node, the system shall generate an error.

[SRS 91] When the filter operation is complete, the following shall be true:

a. The node table shall display nodes that meet the filter criteria.
b. The relationship table shall display relationship that meet the filter criteria.
c. The nodes configuration in graphical format section shall display nodes that meet the filter criteria.

[SRS 92] When the user selects the “edit node” operationwith a node selected, the system shall enable the user to edit the selected node.

[SRS 93] When the user selectsthe “edit node” operationwithout selecting a node, the system shall generate an error.

[SRS 94] When the user selectsthe “edit relationship” operationwith a relationship selected, the system shall enable the user to edit the selected node.

[SRS 95] When the user selectsthe “edit node” operationwithout selecting a relationship, the system shall generate an error.

[SRS 96] When the user selectsthe “export” operationwith an export format selected, the system shall generate an image of the graph in the selected format.

[SRS 97] When the user selectsthe “undo” operation, the system shall undo the changes to a graph since the last commit.

[SRS 98] When the user selectsthe “commit” operation, the system shall save the changes to permanent storage.

[SRS 99] When a change is made to a graph, the following shall be true:

a. The change shall be saved to temporary storage.
b. The change shall be logged in the change list.

[SRS 100] When a change is made to the icon configuration, the impact of change shall be applied to nodes with the changed icon as the icon type.

[SRS 101] When the user selectsthe “add icon” operation, the system shall add a new row in the icon table.

[SRS 102] When the user selectsthe “delete icon” operationwith a selected row in the icon table, the following shall be true:

a. The selected row shall be removed from the icon table.
b. Node with the deleted icon as the icon type shall use the default as the icon type.

[SRS 103] If nodes in a graph have not been repositioned by the user, the following properties of the positioning of the nodes shall be true:

a. The ordering of the nodes shall be in a chronological order determined by the timestamp of each node.
b. The orientation of the nodes shall adhere to the timeline orientation.
c. The proximity of the nodes shall be determined by the interval units and interval.

[SRS 104] When the repositioning of a node in a graph is complete, the node shall be positioned in a user-selected coordinates.

3.3. Non-behavioral Requirements

This section describes performance, availability, and usability requirements of the system.

TBD

&