**Prevent, Mitigate, and Recover (PMR) Insight**

Collective Knowledge System (PICK)

Test plan

Version 1.3

05/06/2020

Document Control

Approval

The Guidance Team and the customer shall approve this document.

Document Change Control

|  |  |
| --- | --- |
| Initial Release: | 1.0 |
| Current Release: | 1.3 |
| Indicator of Last Page in Document: | & |
| Date of Last Review: | 05/06/2020 |
| Date of Next Review: | 05/14/2020 |
| Target Date for Next Update: | 05/20/2020 |

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:

Hector Dozal

Victor Vargas

Eduardo Lara

Irvin Bosquez

Gerardo Armenta

Change Summary

The following table details changes made between versions of this document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Modifier | Description |
| 1.0 | 4/14/2020 | Victor, Irvin, Eduardo | Progress in the section 1, 2, 3 & 4 |
| 1.1 | 4/25/2020 | Gerardo Armenta, Irvin Bosquez | Completed section 5 & 8 |
| 1.2 | 4/27/2020 | Victor Vargas, Eduardo Lara, Hector Dozal | Completed sections 3 & 4. Finished Section 6. |
| 1.3 | 5/6/2020 | Gerardo Armenta | Added introduction to section 2, 3 and Appendix.  Reviewed and Revised document. |

Note: The template presented in this document was taken from:

Donaldson, S., and S. Siegel, *Successful Software Development*. Upper Saddle River, NJ: Prentice Hall, 2001, pp. 321-323.

Note: The template presented in this document was taken from: Donaldson, S., and S. Siegel, *Successful Software Development*. Upper Saddle River, NJ: Prentice Hall, 2001, pp. 321-323 and modified by Humberto Mendoza and Steve Roach.

Supplementary information is from:

Pfleeger, S. *Software Engineering, Theory and Practice*. Upper Saddle River, NJ: Prentice Hall, 1998, p. 365.

**Table of Contents**

[Document Control ii](#_Toc38970226)

[Approval ii](#_Toc38970227)

[Document Change Control ii](#_Toc38970228)

[Distribution List ii](#_Toc38970229)

[Change Summary ii](#_Toc38970230)

[1. Introduction 1](#_Toc38970231)

[1.1. Purpose 1](#_Toc38970232)

[1.2. Scope 1](#_Toc38970233)

[1.3. System Overview 1](#_Toc38970234)

[1.4. Suspension and Exit Criteria 1](#_Toc38970235)

[1.5. Document Overview 2](#_Toc38970236)

[1.6. References 2](#_Toc38970237)

[2. Test Items and Features 3](#_Toc38970238)

[3. Testing Approach 4](#_Toc38970239)

[4. Test XX 5](#_Toc38970240)

[4.1. Test LFI I1 5](#_Toc38970241)

[4.2. Test LFI I2 7](#_Toc38970242)

[4.3. Test LFI I3 9](#_Toc38970243)

[4.4. Test GI I1 12](#_Toc38970244)

[4.5. Test GI I2 16](#_Toc38970245)

[4.6. Test GI I3 20](#_Toc38970246)

[4.7. Test GI I4 24](#_Toc38970247)

[4.8. Test GI I5 28](#_Toc38970248)

[4.9. Test OSR I1 31](#_Toc38970249)

[5. User Interface Testing 35](#_Toc38970250)

[6. Test Schedule 47](#_Toc38970251)

[7. Other Sections 48](#_Toc38970252)

[8. Appendix 49](#_Toc38970253)

[8.1. Analysis of Cleansed Files for Test LFI I1 49](#_Toc38970254)

[8.2. Analysis of Validation and Ingestion for Tests LFI I2 and I3 49](#_Toc38970255)

[8.3. Analysis of Adding Nodes for test GI I1 49](#_Toc38970256)

[8.4. Analysis of Moving Nodes for test GI I2 49](#_Toc38970257)

[8.5. Analysis of Creating Relationships between Nodes for Test GI I3 49](#_Toc38970258)

[8.6. Analysis of Adding and Deleting Nodes for Test GI I4 and I5 49](#_Toc38970259)

[8.7. Analysis of Running PICK on Kali Operating System for test OSR I1 49](#_Toc38970260)

# Introduction

The PMR Insight Collective Knowledge (PICK) tool is the system to be tested for in this document. All test cases provided will be either confirmed to be working or to have failed the test. Below you will find the following test to be performed, along with what the expected results are, and the team members who will be conducting the tests.

## Purpose

The main purpose of this document is to provide a proper guideline to test the software and deliver a functional project to the clients. Also, we are trying to identify the faults and errors that the project PICK that can contain.

This document will focus on the project PICK and it is a Project Test Plan, meaning it will focus on testing the project in general, specifying different parts of it in the different test suites. It contains different test suites focusing on different functionalities of the project, test cases and their descriptions, and a testing schedule.

## Scope

We will be testing a PMR Insight Collective Knowledge (PICK) tool to facilitate the process of writing reports by the White Team (LSH) about the ability of the blue team to defend against cyber-attacks by the red team. This software’s primary goal will consist of facilitating the job of the white team by employing different tools including: Sorting by chronological order based on the date of ingestion, automatic creation of a graphs to better represent when an attack has occurred, creation of vectors to organize all log files that pertain to a singular event, as well as other requirements described within this document. Our system shall focus firstly on improving the analysis of log files, our system shall not use the internet in any way to ensure the security of the system. The success of this project will be determined by the benefits given to the White team upon using this system.

## System Overview

The system that is being exercised is a PMR Insight Collective Knowledge (PICK) tool to facilitate the process of writing reports by the White Team (LSH) about the ability of the blue team to defend against cyber-attacks by the red team. This software’s primary goal will consist of facilitating the job of the white team by employing different tools including: Sorting by chronological order based on the date of ingestion, automatic creation of a graphs to better represent when an attack has occurred, creation of vectors to organize all log files that pertain to a singular event, as well as other requirements described within this document. The system’s functionalities being tested are mainly the ingestion and cleansing of log files; the graphing functionalities and other functions that pertain to the main goal of facilitating analysis.

## Suspension and Exit Criteria

For suspension criteria, we will suspend testing if 50% or more of the critical tests fail, and if 60% or more of the non-critical test fail. For exit criteria we will set the requirement that all critical tests must pass and 80% or more of the non-critical tests must pass.

## Document Overview

The remainder of this test plan document will go into greater detail about the test plan. Section 2 will describe the test items and features, which includes (components, classes, function or methods), to be tested. Section 3 will describe the testing approach that will be used to test the system. It will describe the types of tests that will be performed for each system function one by one and label the criticality of each test case. Section 4 will document test input, specific test procedures, and outcomes for each specified test case. Section 5 will describe user interface testing by detailing the tests by how the user will interact with the system. Section 6 describes the test plan schedule, which will show the members who will be in charge of specific test completions by a certain date. Section 7 explains other test sections that are used to detail the test plan document in greater detail. Section 8 is the appendix and in there will be more detailed results from specific tests that were done throughout the test plan.

## References

[1] E. Tai-Ramirez & S. Roach, SRS\_v7. Internet: <https://github.com/CS4311-spring-2020/pick-tool-team06-team-404/blob/master/doc/SRSv7.pdf>, 2020 (Jan. 30, 2020).

# Test Items and Features

The following items are the ones that are going to be tested for in this document. Our team will be focusing on the main integral parts of the system to test, which includes log ingestion, conversion on logs into nodes, and ability to modify and create relationships between nodes in graphical and table formats. Each parts of the system to be tested has certain features associated to that part and will be tested as well.

|  |  |  |
| --- | --- | --- |
| **TEST ITEMS, FEATURES & COMPONENTS** | | |
| **Test Item** | **Features** | **Components** |
| Log Ingestion | Cleansing | Analysis Subsystem |
| Log Ingestion | Validating | Analysis Subsystem |
| Log Ingestion | Ingesting | Analysis Subsystem and Splunk Subsystem |
| Nodes | Log Entry into Node | Documentation Subsystem and Visual Subsystem |
| Graph Interaction | Modify Nodes | Visual Subsystem and Realtime Actualization Subsystem |
| Graph Interaction | Relationship Between Nodes | Visual Subsystem and Realtime Actualization Subsystem |

# Testing Approach

The following tables show the test suites created to test the system. Theses test suites demonstrate the objectives of the test and importance by either being critical or not. The table’s format is as follows:

* The title of the Test Suite
* The description of the Test suite
* Test Case Identifier
* The objective of each test
* And how critical a test is for the Test Suite.

The title of the Test Suite is the test item to be tested. The description provides what the test item is supposed to do while the test case identifier is used to identify each of the different elements tested. The objective is the components tested that form part of the test item and criticality describes if the objective is critical or not.

Table 1: Test Plan

|  |  |  |
| --- | --- | --- |
| **TEST SUITE <Log File Ingestion>** | | |
| **Description of Test Suite** | **Used to test if log files from directories are ingested into the system without any errors** | |
| **Test Case Identifier** | **Objective** | **Criticality** |
| LFI I1 | **Cleanse log files** | **Critical** |
| LFI I2 | **Validate log files** | **Critical** |
| LFI I3 | **Ingest log files** | **Critical** |

Table 2: Test Plan

|  |  |  |
| --- | --- | --- |
| **TEST SUITE <Graph Interaction>** | | |
| **Description of Test Suite** | **Used to test some utilities about the graph whenever it is created.** | |
| **Test Case Identifier** | **Objective** | **Criticality** |
| GI I1 | **Graph Nodes are created** | **Critical** |
| GI I2 | **Graph availability to move** | **Not Critical** |
| GI I3 | **Accept relationships between Nodes** | **Critical** |
| GI I4 | **Add New Node to graph** | **Not Critical** |
| GI I5 | **Delete Nodes from graph** | **Not Critical** |

Table 3: Test Plan

|  |  |  |
| --- | --- | --- |
| **TEST SUITE<Operating System Run>** | | |
| Description of Test Suite | Used to test software in Kali distribution. | |
| Test Case Identifier | Objective | Criticality |
| OSR I1 | PICK runs in Linux Kali | Critical |

# Test XX

The purpose of this section is to list every test case we plan to do on the system and explain in detail the steps to complete the test. Also, there will be an expected output that the system must get, depending on that output the result of the test will either be a pass or fail. If a test case has yet to be conducted, it will be pending.

## Test LFI I1

**Objective:** The objective of this test is to verify that the system performs cleansing on the log files before ingesting.

**Notes:** Log files are supposed to be cleansed and validated before being ingested into the system, this test will make sure the log files are all cleansed and ready for validation.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test No.: LFI I1 | | | | Current Status: Passed | | |
| Test title: Cleanse log files to prepare them to be ingested | | | | | | |
| Testing approach: This test will be conducted using directories with different log files in a directory folder. Results will be viewed after cleansing is done. | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | | EXEPCTED RESULTS | COMMENTS |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | | The PICK system starts, and the Team Configuration window shows | One should properly complete the Team Configuration, we will assume that is done correctly. |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | | Files are cleansed and a window prompting to continue with validation appears. At this point, files are cleansed, and errors are separated for future showing. |  |
| Concluding Remarks: Cleansing script that was created is working well and removing all unwanted characters in a log file | | | | | | |
| Testing Team:  Hector Dozal | | | Date Completed:  04/14/2020 | | | |

## Test LFI I2

**Objective:** The objective of this test is to verify that the system performs the validation of log files before ingesting to Splunk.

**Notes:** Parts of this process are assumed to be done correctly for the sake of the tests, such as the configurations. Test will make sure files are validated and ready to ingest.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test No.: LFI I2 | | | Current Status: Pending | | | |
| Test title: Validate log files to prepare them to be ingested | | | | | | |
| Testing approach: This test will be conducted using directories with different log files in a directory folder. Results will be viewed after validating is done. | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | EXEPCTED RESULTS | COMMENTS | |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. | |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. | |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. | |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | Files are cleansed and a window prompting to continue with validation appears. |  | |
| 5 | Click on “Validate” button | This will start the validation process | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  | |
| Concluding Remarks: | | | | | |
| Testing Team:  Victor Vargas | | | Date Completed:  04/29/2020 | | |

## Test LFI I3

**Objective:** The objective of this test is to verify that the system performs the ingestion into Splunk properly

**Notes:** Parts of this process are assumed to be done correctly for the sake of the tests, such as the configurations. Test will make sure files are ingested to Splunk.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test No.: LFI I3 | | | Current Status: Passed | | |
| Test title: Ingest Log Files to Splunk | | | | | |
| Testing approach: This test will be conducted by going through the configurations and starting the ingestion process for files in the folders. | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | EXEPCTED RESULTS | COMMENTS |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | Files are cleansed and a window prompting to continue with validation appears. |  |
| 5 | Click on “Validate” button | This will start the validation process | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  |
| Concluding Remarks:  The system accurately ingests log files from the directories into Splunk | | | | | |
| Testing Team:  Victor Vargas | | Date Completed:  04/15/2020 | | | |

## Test GI I1

**Objective:** The objective of this test is to verify that it is possible to add nodes to the graph from a defined vector

**Notes:** We will assume previous steps have been done and we are in the related tabs.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test No.: GI I1 | | | Current Status: Passed | | |
| Test title: Add Nodes to Graph from Vector | | | | | |
| Testing approach: This test will be conducted in the Table View tab, the Graph view tab, and the split view tab. | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | EXEPCTED RESULTS | COMMENTS |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | Files are cleansed and a window prompting to continue with validation appears. |  |
| 5 | Click on “Validate” button | This will start the validation process | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  |
| 7 | The user clicks on the Graph View, the Table View or the Split View tab. | The purpose is to enter one of the views that supports the add node functionality. | | The proper tab is opened. | We assume the user starts here, having done the configuration and with the program having ingested files already. |
| 8 | The user selects a vector to view. | Convert vector leg entries into nodes to generate a graph | | Nodes have been created from the vector log entries and formed a graph | Here both a row and a node are equivalent, just different representations. |
| Concluding Remarks:  The system creates a graph of nodes from vector log entries | | | | | |
| Testing Team:  Eduardo Lara, Irvin Bosquez | | Date Completed:  04/27/2020 | | | |

## Test GI I2

**Objective:** The objective of this test is to verify that it is possible to move Nodes

**Notes:** We will assume previous steps have been done and we are in the related tabs.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test No.: GI I2 | | | Current Status: Passed | | |
| Test title: Move Nodes | | | | | |
| Testing approach: This test will be conducted in the Graph view tab, and the split view tab. | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | EXEPCTED RESULTS | COMMENTS |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | Files are cleansed and a window prompting to continue with validation appears. |  |
| 5 | Click on “Validate” button | This will start the validation process | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  |
| 7 | The user clicks on the Graph View, the Split View tab. | The purpose is to enter one of the views that supports the add node movement functionality. | | The proper tab is opened. | We assume the user starts here, having done the configuration and with the program having ingested files already. |
| 8 | The user clicks on the “Add Node” button. | Trigger the event of adding a Node | | A Node is added to the graph, and a Row is added to the Table view. | Here both a row and a node are equivalent, just different representations. |
| 9 | The user selects the Node, by clicking on it. | This is to select the Node to do operations on it | | The Node is selected |  |
| 10 | The user clicks and holds the selected Node and slides the cursor to move Node | This is to trigger the action of moving the Node | | The Node moves properly. |  |
| Concluding Remarks:  The system is able to allow nodes to move within the graph | | | | | |
| Testing Team:  Eduardo Lara, Irvin Bosquez | | Date Completed:  04/20/2020 | | | |

## Test GI I3

**Objective:** The objective of this test is to verify that it is possible to create relationships between nodes on the graph with the graphing interface.

**Notes:** We will assume previous steps have been done and we are in the related tabs.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test No.: GI I3 | | | | Current Status: Pending | | | |
| Test title: Create Relationship between Nodes from Graph | | | | | | | |
| Testing approach: This test will be conducted in the Table View tab, the Graph view tab, and the split view tab. | | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | | EXEPCTED RESULTS | COMMENTS | |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. | |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. | |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. | |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | | Files are cleansed and a window prompting to continue with validation appears. |  | |
| 5 | Click on “Validate” button | This will start the validation process | | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  | |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  | |
| 7 | The user clicks on the Graph View, the Table View or the Split View tab. | The purpose is to enter one of the views that supports the add node functionality. | | | The proper tab is opened. | We assume the user starts here, having done the configuration and with the program having ingested files already. | |
| 8 | The user selects a node from the graph | The purpose is to get information on which node user wants to be part of a relationship | | | Node is selected |  | |
| 9 | The user selects “Add Relationship” button | Trigger the event of creating a relationship | | | The selected node is then awaiting the second node to be selected |  | |
| 10 | The user selects a second Node from the graph | To create a relationship between two nodes on the graph | | | Both selected nodes now have a relationship between them and an edge will be shown on the graph to see this relationship visually |  | |
| Concluding Remarks:  The system deletes a node from the graph | | | | | | |
| Testing Team:  Eduardo Lara, Irvin Bosquez | | | Date Completed:  04/30/2020 | | | |

## Test GI I4

**Objective:** The objective of this test is to verify that it is possible to add new nodes to the graph with the graphing interface.

**Notes:** We will assume previous steps have been done and we are in the related tabs.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test No.: GI I4 | | | | Current Status: Passed | | | |
| Test title: Add New Nodes to Graph | | | | | | | |
| Testing approach: This test will be conducted in the Table View tab, the Graph view tab, and the split view tab. | | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | | EXEPCTED RESULTS | COMMENTS | |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. | |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. | |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. | |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | | Files are cleansed and a window prompting to continue with validation appears. |  | |
| 5 | Click on “Validate” button | This will start the validation process | | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  | |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  | |
| 7 | The user clicks on the Graph View, the Table View or the Split View tab. | The purpose is to enter one of the views that supports the add node functionality. | | | The proper tab is opened. | We assume the user starts here, having done the configuration and with the program having ingested files already. | |
| 8 | The user clicks on the “Add Node” button. | Trigger the event of adding a Node | | | A Node is added to the graph, and a Row is added to the Table view. | Here both a row and a node are equivalent, just different representations. | |
| Concluding Remarks:  The system creates a new node into the graph | | | | | | |
| Testing Team:  Eduardo Lara, Irvin Bosquez | | | Date Completed:  04/19/2020 | | | |

## Test GI I5

**Objective:** The objective of this test is to verify that it is possible to add new nodes to the graph with the graphing interface.

**Notes:** We will assume previous steps have been done and we are in the related tabs.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test No.: GI I5 | | | | Current Status: Passed | | | |
| Test title: Delete Nodes from Graph | | | | | | | |
| Testing approach: This test will be conducted in the Table View tab, the Graph view tab, and the split view tab. | | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | | EXEPCTED RESULTS | COMMENTS | |
| 1 | Start the PICK Software | This will start the environment to test the cleansing | | | The PICK system starts, and the Team Configuration window shows | One should fill the Team Configuration properly; we will assume that is done correctly. | |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | | The PICK system displays the Event Configuration Window | Again, we will assume this section is filled properly. | |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. | |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | | Files are cleansed and a window prompting to continue with validation appears. |  | |
| 5 | Click on “Validate” button | This will start the validation process | | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  | |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown |  | |
| 7 | The user clicks on the Graph View, the Table View or the Split View tab. | The purpose is to enter one of the views that supports the add node functionality. | | | The proper tab is opened. | We assume the user starts here, having done the configuration and with the program having ingested files already. | |
| 8 | The user selects a node from the graph | The purpose is to get information on which node user wants to be deleted | | | Node is selected |  | |
| 9 | The user selects “Delete Node” button | Trigger the event of deleting a Node | | | The selected node is then deleted from the graph view and the table view. | Here both a row and a node are equivalent, just different representations. | |
| Concluding Remarks:  The system deletes a node from the graph | | | | | | |
| Testing Team:  Eduardo Lara, Irvin Bosquez | | | Date Completed:  04/27/2020 | | | |

## Test OSR I1

**Objective:** Verify program runs as intended in the operating system Kali.

**Notes:** We will assume all software needed to run in Kali OS has been downloaded and is running.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test No.: OSR I1 | | | | Current Status: Failed | | |
| Test title: PICK Kali | | | | | | |
| Testing approach: This test will be conducted by using the pick system that has been designed to run in Kali | | | | | | |
| STEP | OPERATOR ACTION | PURPOSE | | | EXEPCTED RESULTS | COMMENTS |
| 1 | The user initiates PICK software. | This starts PICK and shows the main window. | | | The PICK system is up and running waiting for user input. |  |
| 2 | The user clicks on File, then clicks on New. | This will open the Team Configuration to start a new project. | | | The PICK system starts, and the Team Configuration window shows | We assume the user enters the information in the Team Configuration. |
| 2 | Go to Event Configuration by Pressing “Event Configuration” Button | This will change to the Event Configuration Window | | | The PICK system displays the Event Configuration Window | We assume the user entered all the information correctly. |
| 3 | Go to Directory Configuration by Pressing “Directory Configuration” button | This will change to the Directory Configuration Window | | | The PICK system displays the Directory Configuration Window | We assume this section is filled properly as it does not pertain to the test. |
| 4 | Click on “Start Ingestion” button | This will start the cleansing and validation process on the files in the directories selected. | | | Files are cleansed and a window prompting to continue with validation appears. At this point, files are cleansed, and errors are separated for future showing. |  |
| 5 | Click on “Validate” button | This will start the validation process | | | A window prompting the user to continue with ingestion will appear. At this point entries are validated, and errors saved for future reference. |  |
| 6 | Click on “Ingest” to begin ingestion. | Proceeds to ingest files to Splunk. | | | Splunk will be populated with the proper Events/Entries. The main PICK window is shown | Splunk error. The system found no files in Splunk. |
| 7 | Go through and click on every “tab” | Check if every tab is functioning on Kali | | | Each “tab” does what it is supposed to do with the previous version, but on Kali with no errors. | All tabs where checked to make sure all sections in PICK were working. After file ingestion, the system crashes as it can’t find log files from Splunk. |
| Concluding Remarks:  PICK system was not able to work in the Kali environment all the time. While it did manage to work in some instances, it is not what is desired. There might possibly be an issue with Splunk changing from enterprise to free and vice versa. | | | | | | |
| Testing Team:  Gerardo Armenta | | | Date Completed:  04/27/2020 | | | |

# User Interface Testing

There are some interfaces in which the user has to interact with the application. We will try to go over some of them. Some of the things that will be tested are the following:

NOTE: Figures used provide context to UI available to the user.

* Maximizing/Minimizing the window
  + Minimizing and maximizing the window does not alter the functionality of the PICK system.

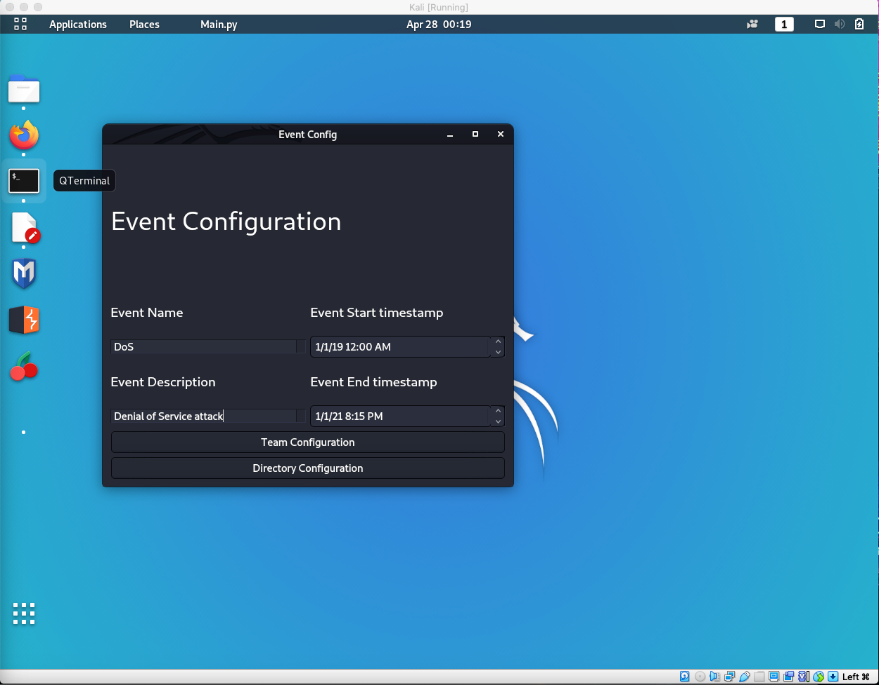


Fig 5.1 Event Configuration in small size

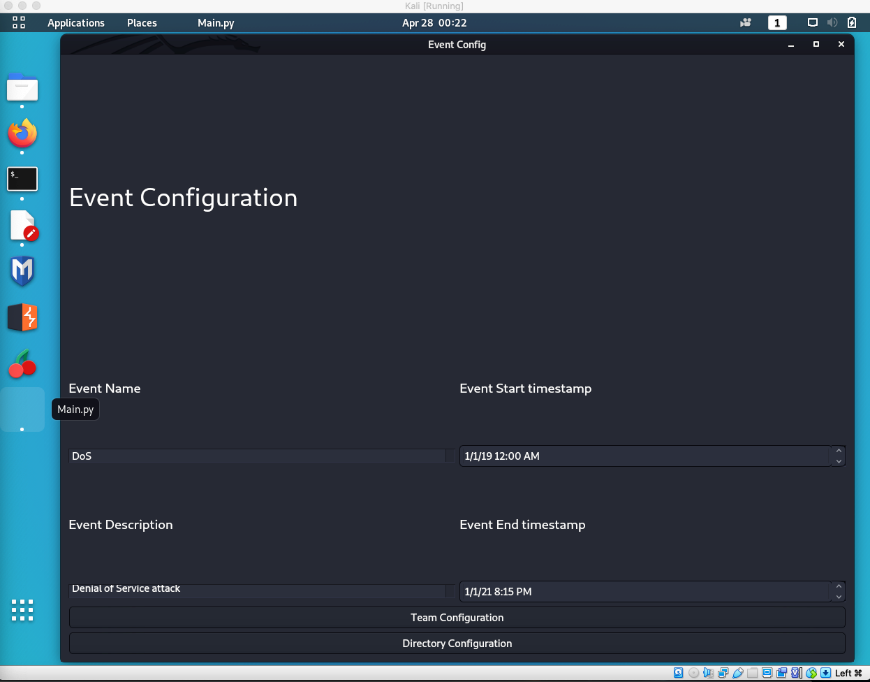


Fig 5.2 Event Configuration made bigger

* Toolbar functions
  + File, Edit/Changes, and View include necessary options.
  + The user can go back to the Event Configuration and Team Configuration at any given time when in the Main Window.

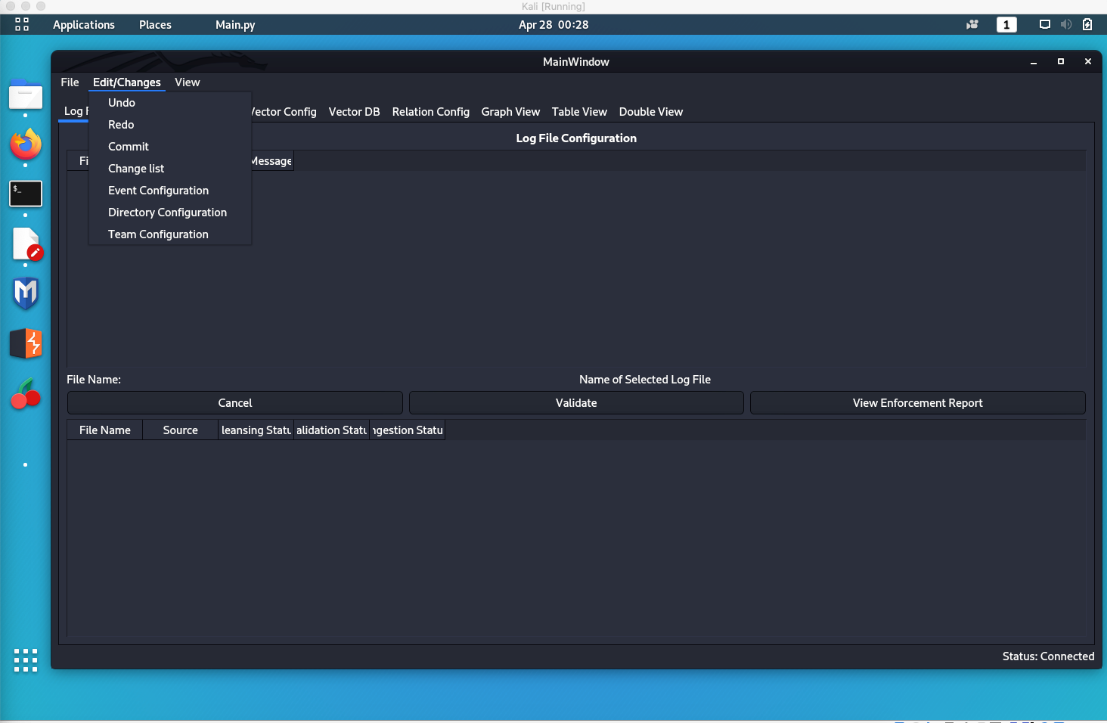


Fig 5.2 Toolbar Edit/Changes options in Log File Config screen

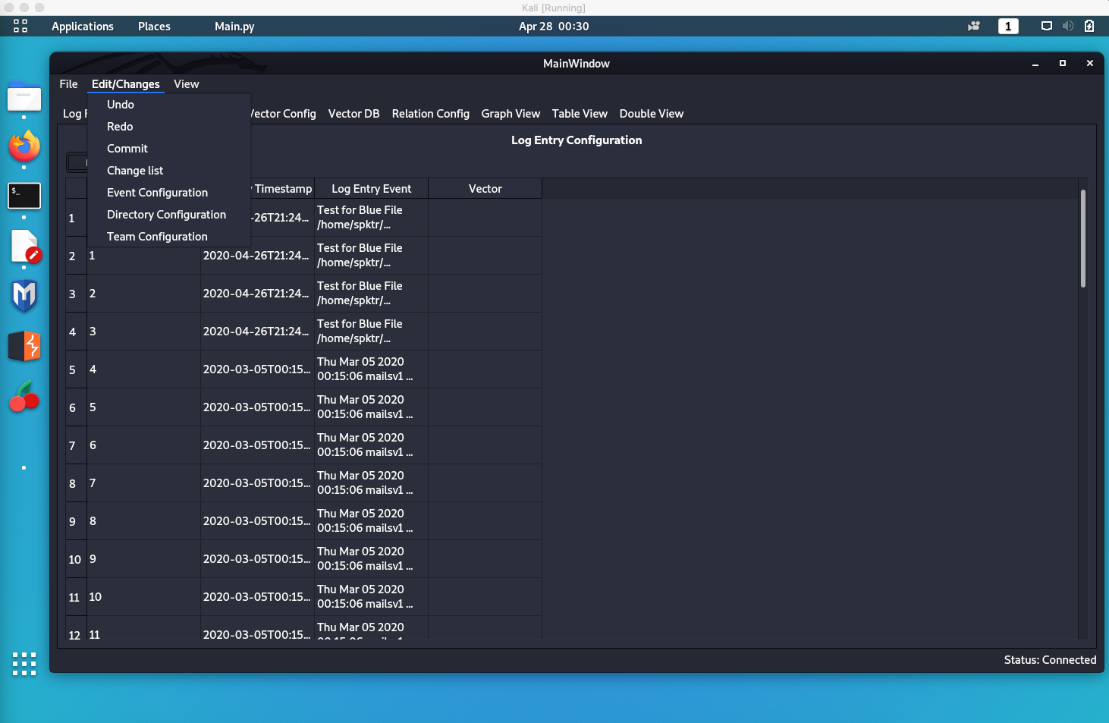


Fig 5.3 Toolbar Edit/Changes options in Log Entry Config screen

* Team Configuration
  + Lead can be entered in the lead section.
  + Clicking connect directs user to the Event Configuration screen.
  + Clicking Directory Configuration directs the user to the Event Configuration screen.

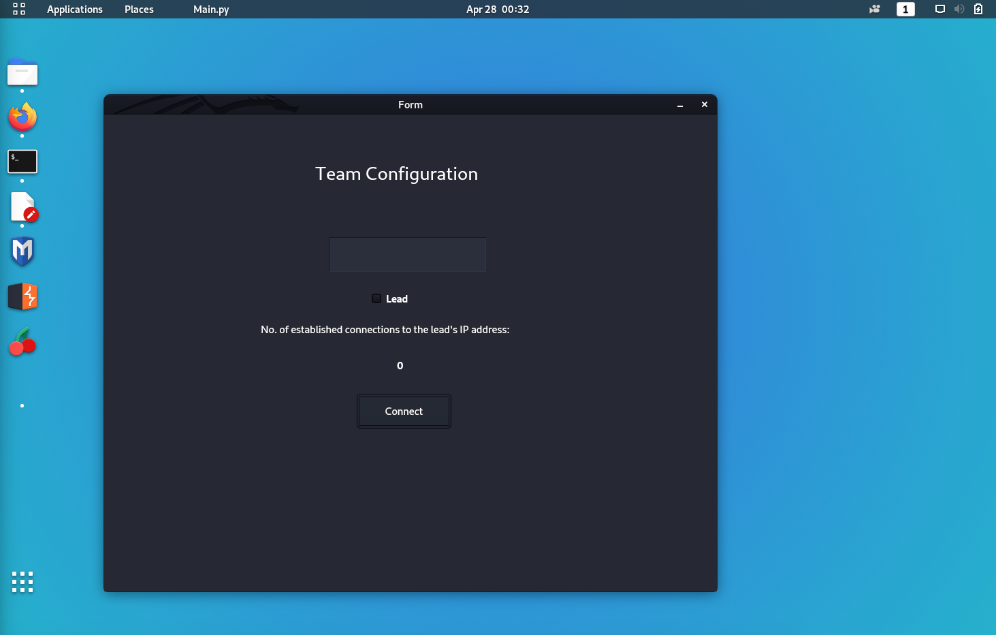


Fig 5.4 Team Config initial screen

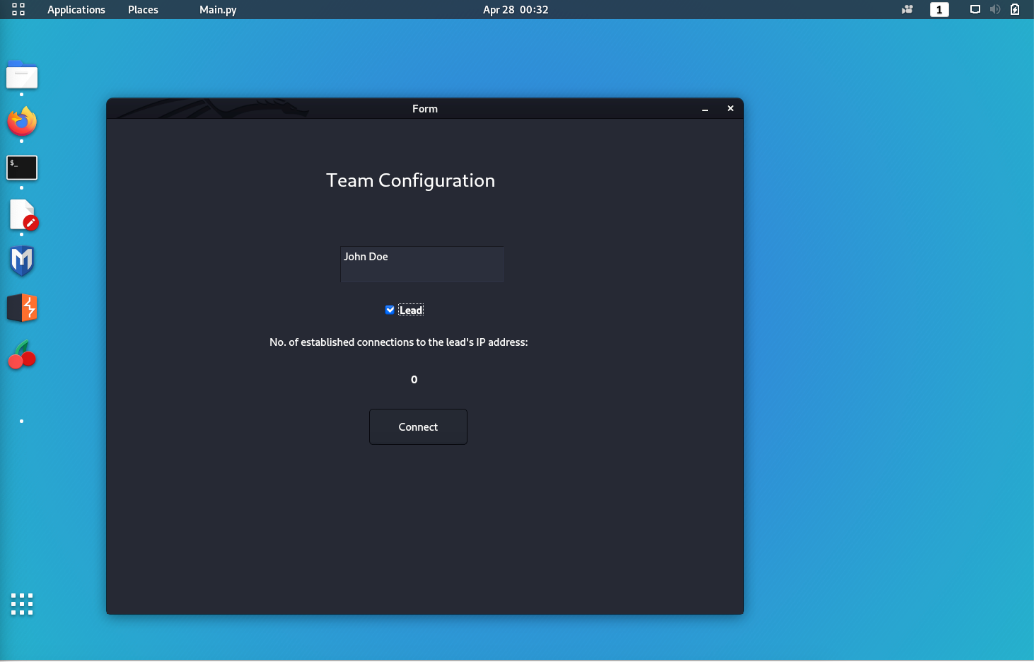


Fig 5.5 Team Config set up for lead

* Event Configuration
  + The event timestamps are preformatted and only accept one format as required.
  + Option for clicking back to Team Configuration directs the user to Team Configuration screen.
  + The event name can be entered in the screen.
  + A description of the event can be added in the configuration.
  + Clicking Directory Configuration checks that the event start timestamp is prior to the event end timestamp and notifies the user if it is in the correct order and proceeds to the Directory Configuration screen.
    - If the event start timestamp is bigger than the end date, an error will pop up letting the user know about the issue and won’t proceed to the Directory Configuration screen.

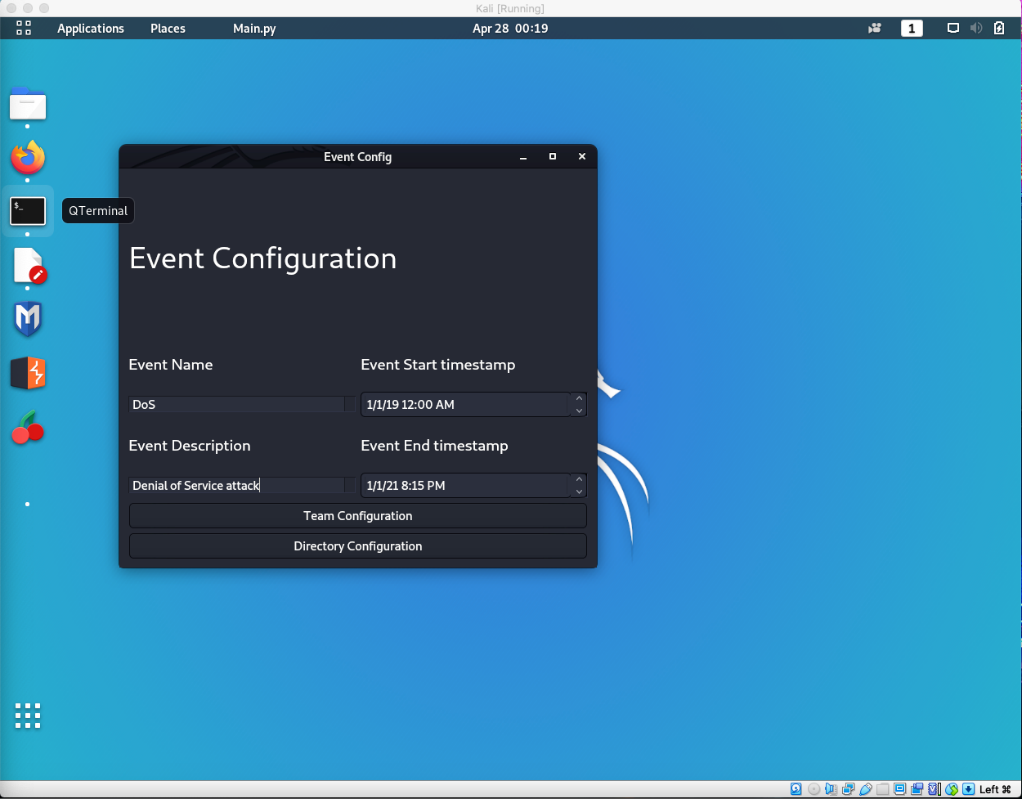


Fig 5.6 Event Configuration in relation to Kali OS display

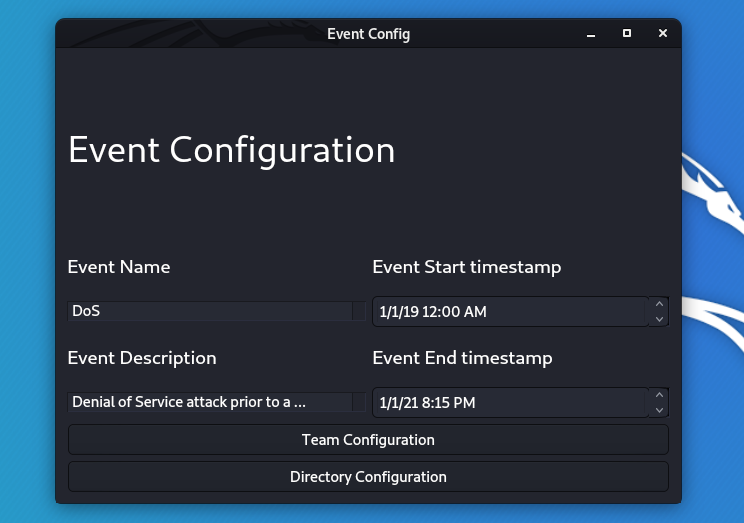


Fig 5.7 Event Configuration in detail completed

* Directory Configuration
  + Option for clicking the Event Configuration button to take the user back to that screen.
  + Clicking Root Directory allows the user to select the path of where the blue, red, and white team folders are by a pop up to the system’s file management directory.
    - If the root directory chosen by the user is not in the appropriate format by having a Red Team Folder, Blue Team Folder, and White Team Folder, a pop up is shown explaining the error and the user must click ok and is prompted the Directory Configuration to reselect the correct root directory.
  + Selecting the appropriate root directory with the correct folder format for the teams and clicking Start Data Ingestion will take the user to the Log File Configuration in the main screen.



Fig 5.8 Directory Configuration pending user input



Fig 5.9 Directory Configuration with Root Directory entered structure met

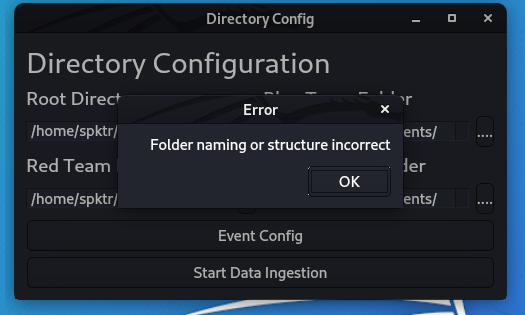


Fig 5.10 Directory Configuration with Root Directory Error

* Main Window
  + The main window is where the following tabs are shown for the user to click on them and take them to the respective screen:
    - Log Entry Config
    - Vector Config
    - Vector DB
    - Relation Config
    - Graph View
    - Table View, and
    - Double View.

The user can go back and forth within the tabs in the screen.

* Log File Configuration
  + The user is presented with the files that failed the cleansing process.
  + Selecting a file will provide the user with the option the validate the file, view enforcement report or cancel the selection.
    - If the user clicks validate, the log file is validated and passed on as a log entry.
    - If the user clicks on view enforcement report, a report is brought up explaining the error message in more detail.
    - Clicking cancel will cancel the selection of a log file.

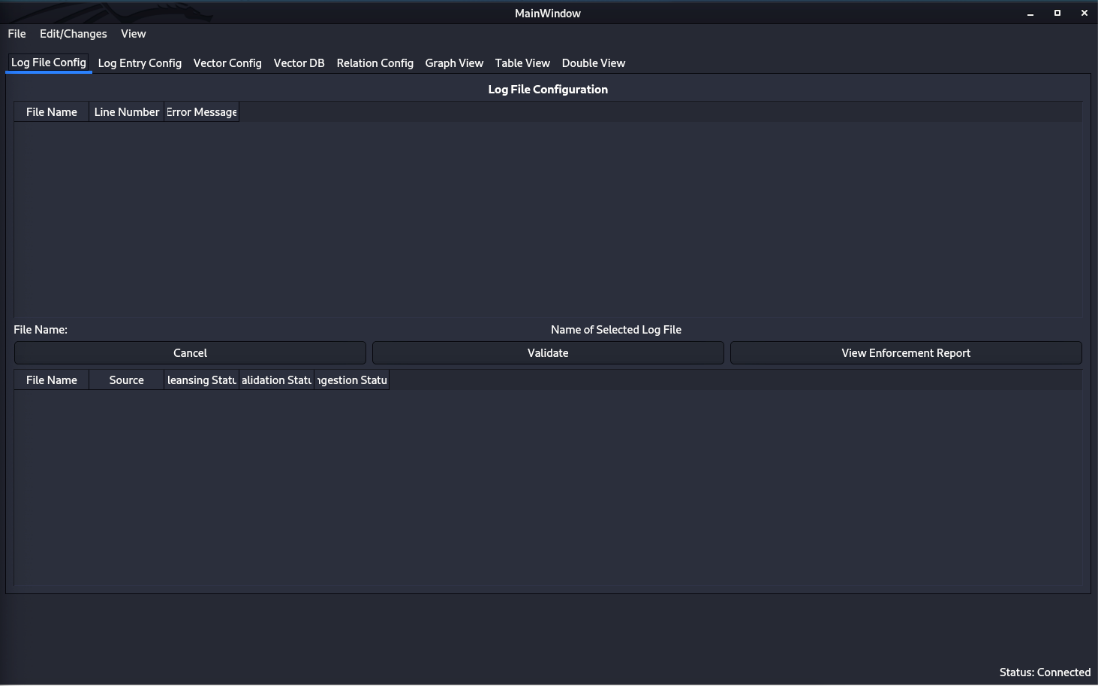


Fig 5.11 Log File Config screen after ingesting

* Log Entry Configuration
  + The user is provided with a list of log entries with the list number, log entry timestamp, log entry event and vector. Clicking any of these sections sorts the list in ascending or descending order.
  + Clicking the Filter button available pops up a window where the user can enter a keyword search or check certain parameters available to filter by creator, event type and/or time.
    - Clicking ok will alter the list by the selected options.
    - Clicking cancel will close the filter configuration pop up and not apply any of the selected options to filter the list.

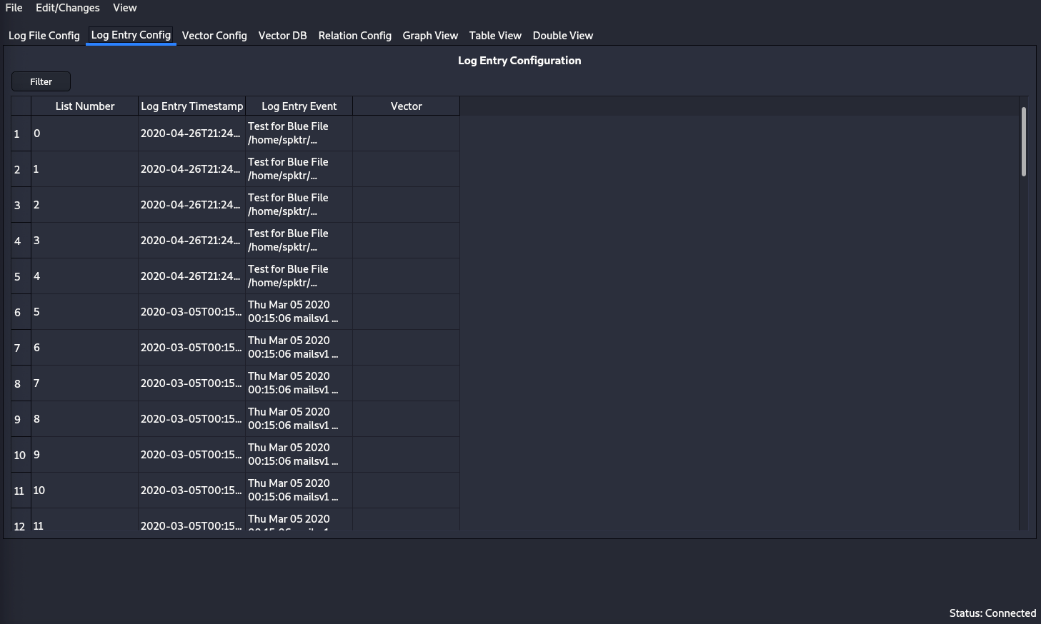


Fig 5.12 Log Entry Config with log files

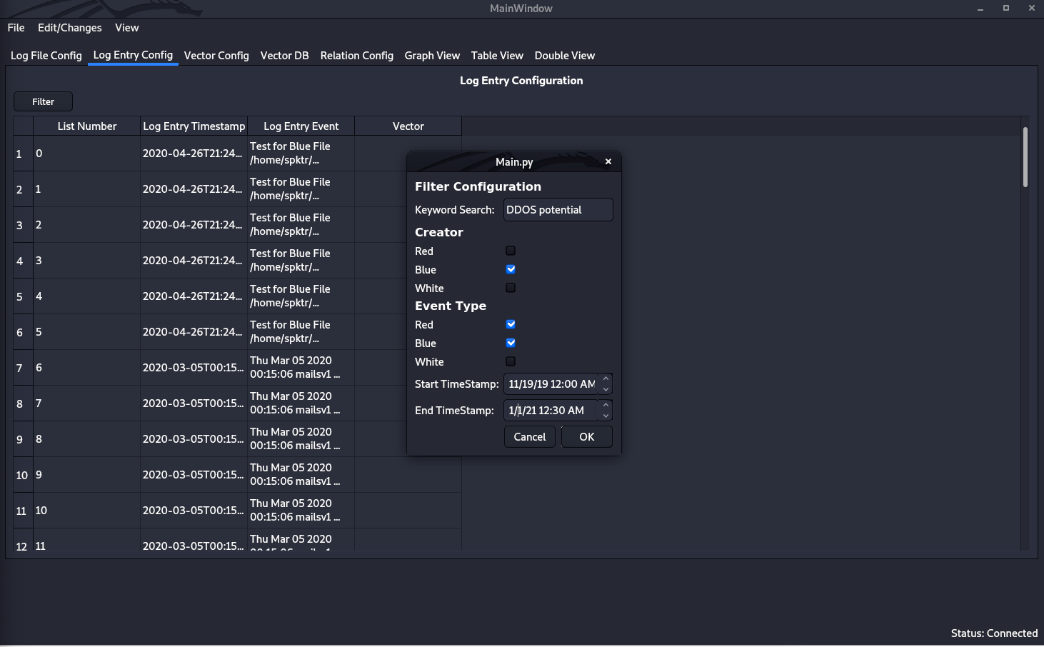


Fig 5.13 Log Entry Config Filter Configuration option

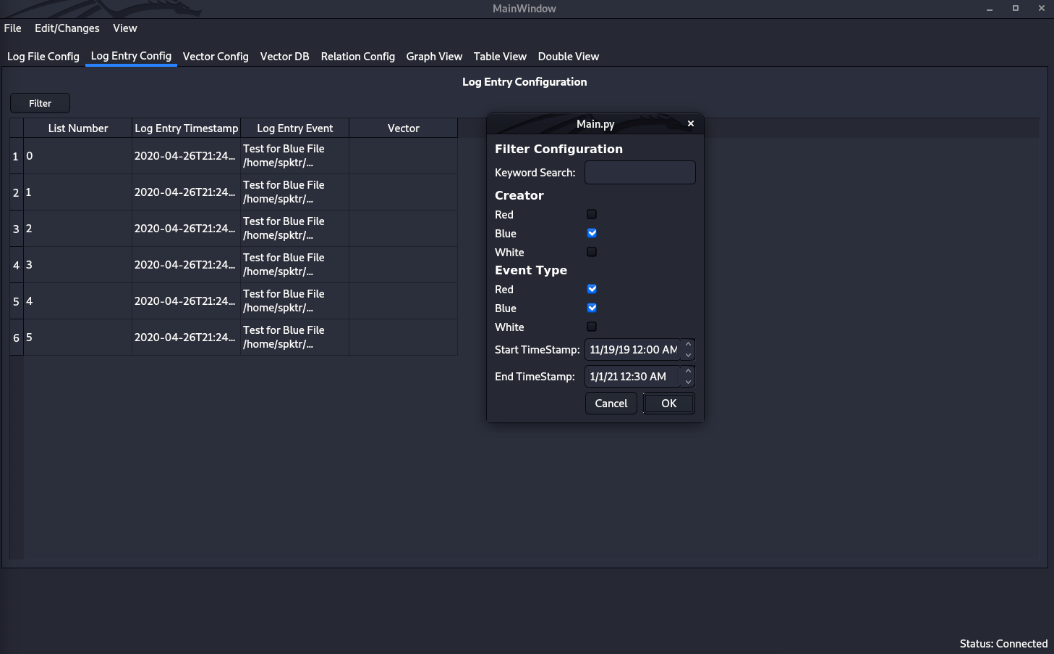
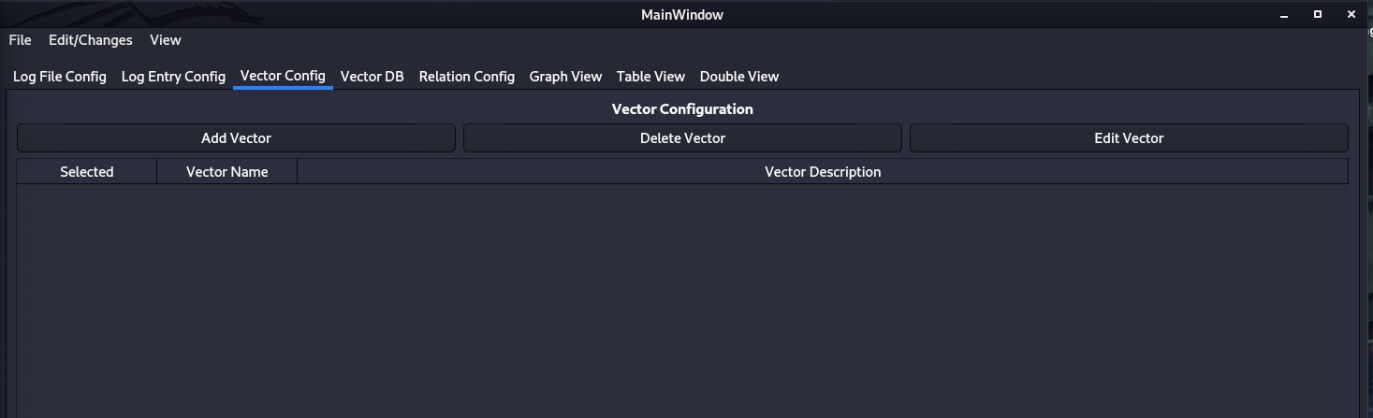


Fig 5.14 Log Entry Config Filter Configuration selected with results

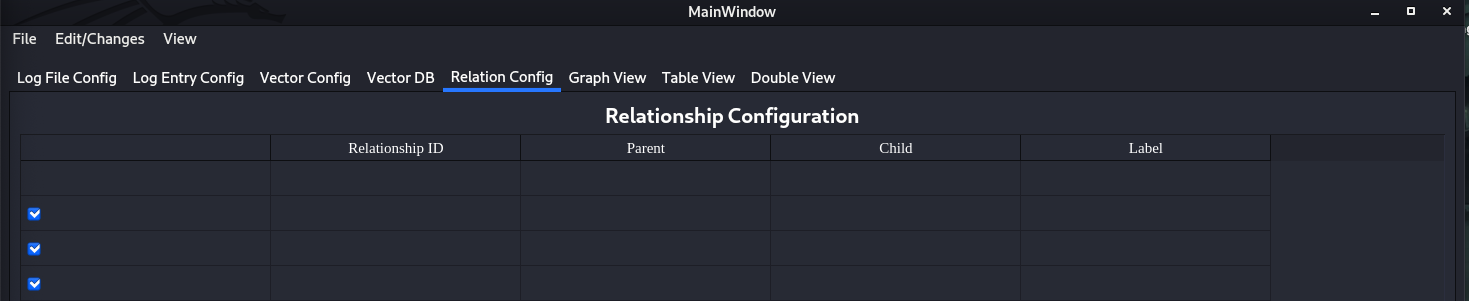
* Vector Configuration
  + The user is presented with the buttons to add vector, delete vector, and edit vector.
  + Clicking on add vector will allow the user to add a new vector by name and adding a description.
  + Clicking on edit vector allows the user to edit a vector previously created.
  + The delete vector button allows the user to delete a vector in the list.

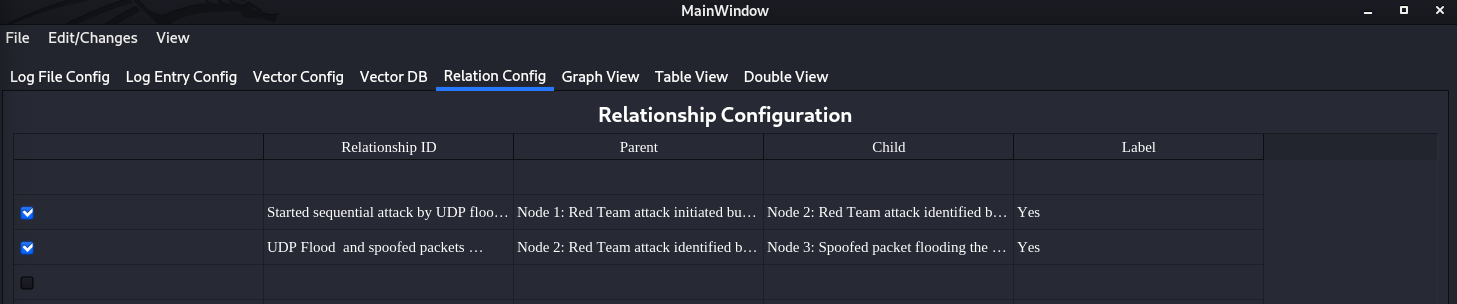
Fig5.15 Vector Configuration screen

* Vector DB
  + Shows the user the Vectors pulled and pushed to the lead.
  + The user can check or uncheck vectors from the tables.

Figure 5.16 Vector DB screen with Pull and Push information

* Relation Configuration
  + Presents the user with the relationships between two nodes. Its Relation ID, the parent, child, and label.
  + The user can mark or unmark the relationship.

Figure 5.17 Relation Configuration clean start

Figure 5.18 Relation Configuration with relationship information for nodes

* Graph View
  + Dead point in which a node can be moved
  + Moving the nodes from graph
  + Adding/Deleting nodes from graph
  + Relationships between nodes

A screenshot of a cell phone

Description automatically generated

Figure 5.19 Graph View

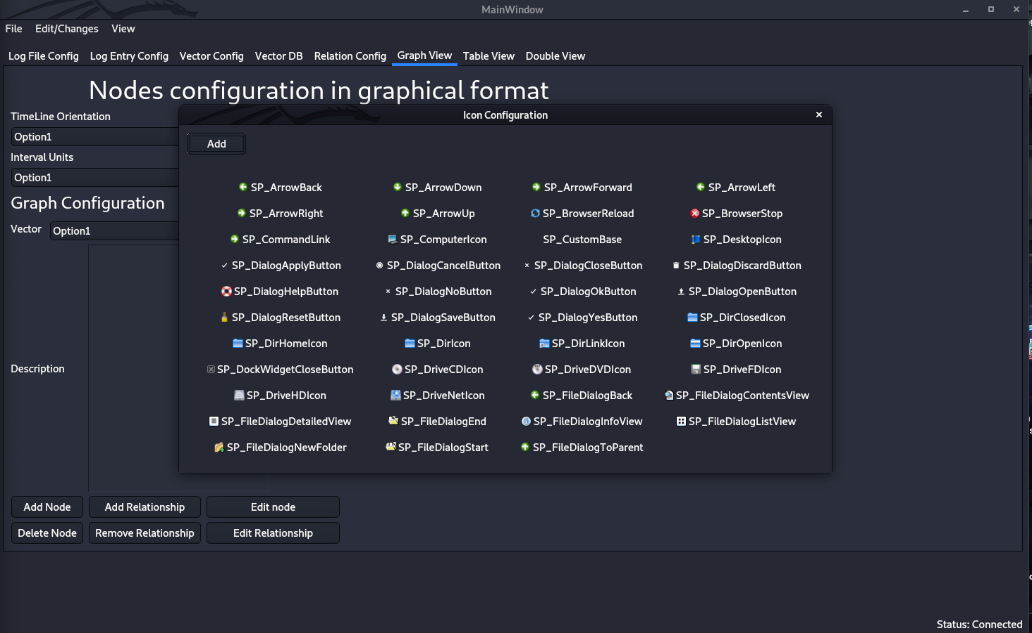
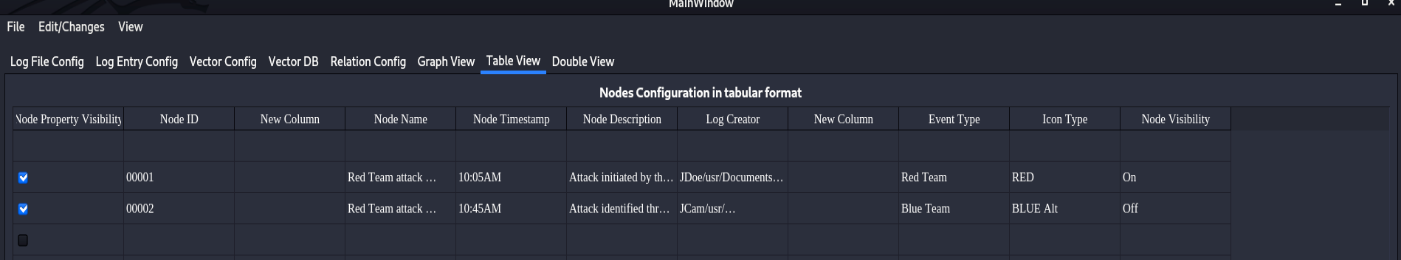


Figure 5.20 Graph View with icon selection tool enabled

* Table View
  + The user can check or uncheck the node visibility from the graph presented in tabular format.

Figure 5.21 Table View

Figure 5.22 Table View with node information in tabular format

* Double View
  + The user will be able to view the nodes in graph view and table view in split screen.

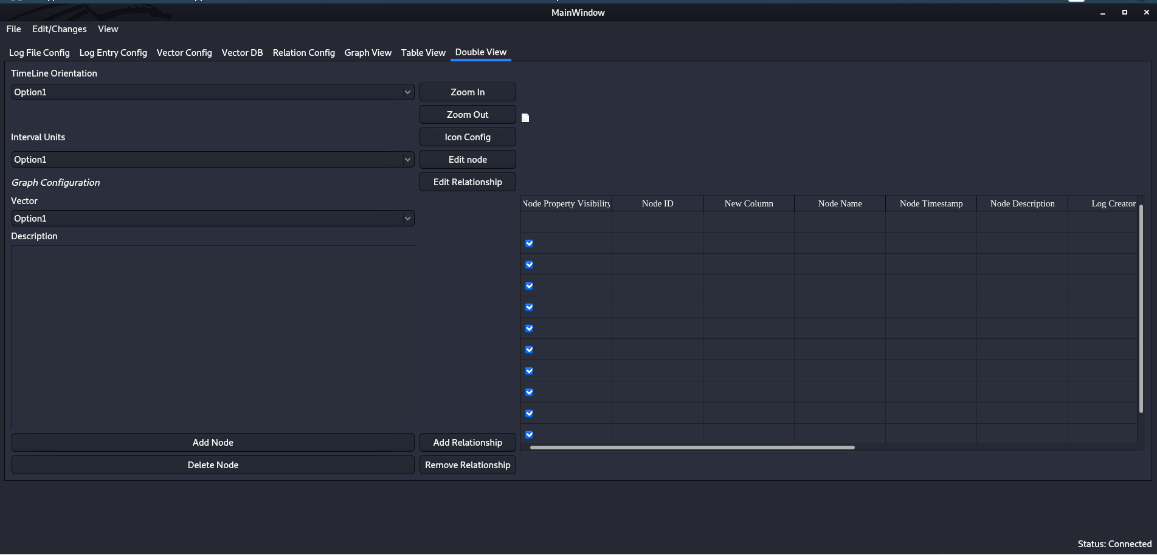


Figure 5.23 Double View

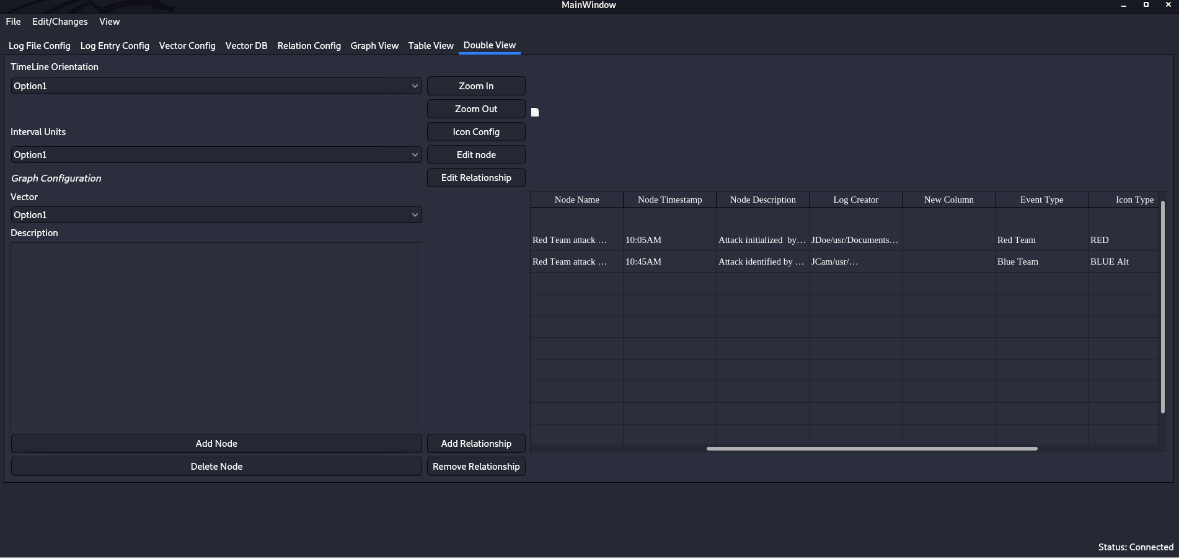


Figure 5.24 Double View with tabular information present

# Test Schedule

Below you will find the following test schedule that will be used to show who will conduct certain tests and what date they are expected to test.

|  |  |  |
| --- | --- | --- |
| **Task and date** | **People** | **Description** |
| LFI I1  04/14/2020 | Hector Dozal | Created Cleansing script to remove unwanted characters from log files |
| LFI I2  04/29/2020 | Victor Vargas | Verify that the system performs the validation of log files before ingesting to Splunk |
| LFI I3  04/15/2020 | Victor Vargas | Verify that the system performs the ingestion into Splunk properly |
| GI I1  04/27/2020 | Irvin Bosquez  Eduardo Lara | Verify that it is possible to add nodes to the graph from a defined vector |
| GI I2  04/20/2020 | Irvin Bosquez  Eduardo Lara | Verify that it is possible to move Nodes |
| GI I3  04/30/2020 | Irvin Bosquez  Eduardo Lara | Verify that it is possible to create relationships between nodes on the graph with the graphing interface |
| GI I4  04/19/2020 | Irvin Bosquez  Eduardo Lara | Verify that it is possible to add new nodes to the graph with the graphing interface |
| GI I5  04/27/2020 | Irvin Bosquez  Eduardo Lara | Verify that it is possible to delete nodes from the graph with the graphing interface |
| OSR I1  04/27/2020 | Gerardo Armenta | Verify program runs as intended in the operating system Kali. |

# Other Sections

<< Other sections that may appear in a test plan (but not required for this course) are:

Test Management Requirements: how testing is to be managed; a delineation of responsibilities of each project organization involved with testing

Staffing and training needs: delineate the responsibilities of those individuals who are to perform the testing, level of skill required, and training to be provided

Environmental Requirements: describe the hardware (including communication and network equipment) needed to support testing; describe configuration of hardware components on which software and database to be tested are to operate.

Software Requirements: describe the software needed to support testing; include the software code and databases that are object of the testing. Also include software tools such as compilers, CASE instruments and simulators that are needed to model the user’s operational environment.

Risk and contingencies

Cost: include an estimate of costs.

Approvals

Test Deliverables

# Appendix

The following shows an in-depth analysis of the expected output from the tests completed. Each test completed includes an evaluation based on what occurred.

## Analysis of Cleansed Files for Test LFI I1

For the evaluation of the cleansing part of the program, one should look at the contents of the file before the cleansing is done, and after the cleansing is done. The evaluation must be directly checking the files since the cleansing is just one step of the process of the program.

## Analysis of Validation and Ingestion for Tests LFI I2 and I3

For the evaluation of the validation and ingestion process the tester shall investigate Splunk to evaluate if the entries were ingested and if they are within the proper event range. Since Splunk will be the tool used for ingestion and storage of the log entries, the evaluation should be done with Splunk and not just the PICK tool.

## Analysis of Adding Nodes for test GI I1

For the evaluation of being able to add nodes, the tester must look at the graph prior to adding a new node and noticing if the new node has been added into the graph, thus creating a new graph with the new node being added to it.

## Analysis of Moving Nodes for test GI I2

For the evaluation of being able to move nodes, one must be able to click a node with the mouse and hold it to drag it into a new position. The node that has been selected must move to the new part of the graph to which the user has let go of the mouse and the node should be in that new position.

## Analysis of Creating Relationships between Nodes for Test GI I3

For the evaluation of being able to create relationships between nodes, one must select a node to be in the relationship, then select the add relationship button, and finally select the second node in the relationship. Once that has been done, an edge representing the relationship will be shown on the graph.

## Analysis of Adding and Deleting Nodes for Test GI I4 and I5

For the evaluation of being able to add nodes, the tester must look at the graph prior to adding a new node and noticing if the new node has been added into the graph, thus creating a new graph with the new node being added to it.

For the evaluation of being able to delete a node, the tester must look at the graph and select the node which they want to delete. Once node is selected, tester selects delete node button and the node should be deleted from the graph.

## Analysis of Running PICK on Kali Operating System for test OSR I1

For the evaluation of PICK’s usability in Kali OS, one must verify that Splunk is running and that the username and password is the same on the software as on Splunk. MongoDB must be running as well so that it can be accessed when running PICK. All of this software runs in conjunction to make PICK work as intended. In further evaluation, the PICK application run in Kali, all other tests where completed to make sure they run as intended in Kali. Unfortunately, between Splunk having two different versions, enterprise and free, it did cause some issues within the system. While building the software and having short runs proofed success, running them in Kali as a complete system caused issues with Splunk by not receiving the ingested logs at times causing the system to crash. Also, the source code must include the local host name appropriate for the Kali system since Kali, by default, asks the user to name the localhost when initially installed.

&