Scenario: End-to-End System Workflow

Precondition: The analyst uses the PICK system to create a visualization of an attack.

The analyst has a predefined directory structure that holds the Red, Blue, and White team directories.

Post-condition: On successful completion, the analyst was able to export a graph created. Project files are saved by the system onto the database.

Actors: Analyst, OCR, Splunk, Audio-Transcriber, & Database

1. Analyst launches the PICK system.
2. System displays welcome screen with options to begin new project, continue local project, connect to project, or exit the system.
3. Analyst selects “Begin New Project” option (ALT 1, ALT 2, ALT 3)
4. The system assigns the analyst as the lead.
5. System displays window comprised of:
   * Event description text field
   * Event start timestamp text field
   * Event end timestamp text field
   * Root directory text field
   * Red team folder name text field
   * White team folder name text field
   * Blue team folder name text field
   * Option with label “next”
6. The analyst inputs event name, event description, event start timestamp, event end timestamp, root directory, red team folder name, white team folder name, blue team folder name.
7. The analyst selects the “start data ingestion” option.
8. The system verifies event configuration information is formatted correctly, and that directories exist. (ALT 4)
9. The system saves event configuration in the database.
10. The system loads file names from directories to determine which parsing solution to use per file based on filetype. (ALT 5, ALT 6)
11. The system cleanses log files (ALT 7)
12. The system connects to Splunk (ALT 8)
13. The system sends log files to Splunk
14. Splunk ingests log files and stores them in its own database
15. The system validates log files (ALT 9)
16. The system generates a report of any errors in the ingestion process for all files.
17. The system displays the enforcement action report in a window comprised of:
    * The report itself
    * An option to continue
    * An option to accept invalid log files
18. The analyst selects the option to continue (ALT 10)
19. The system retrieves log entries of valid log files from Splunk and saves them into the project database
20. The system displays the main window to the analyst.
21. The analyst selects the option to “Add Vector” in the dropdown menu of the main window labeled “Project”
22. The system displays the add vector window comprised of:
    * A text field labeled “vector name”
    * A text field labeled “vector description”
    * An option to cancel
    * An option to accept
23. The analyst provides a name for the vector
24. The analyst provides a description for the vector
25. The analyst selects the option to accept (ALT 11)
26. The system adds a vector entry into the database with the information that the analyst provided
27. The analyst selects the desired log entries to associate with the selected vector.
28. The system associates selected log entries to the vector in the database
29. The system creates nodes with information of the associated log entries and stores them in the database
30. The system displays the nodes in the graph view and table view of the main window
31. The analyst selects nodes to hide in the graph view (ALT 12)
32. The system changes the selected nodes’ visibility to false and hides the nodes in the graph view
33. The analyst selects “Add Relationship” option from the Graph right-click drop-down menu (ALT 13)
34. The system displays the add relationship window comprised of:
    * A text field labeled “child node ID”
    * A text field labeled “parent node ID”
    * A text field labeled “relationship label”
    * An option to cancel
    * An option to accept
35. The analyst provides the child node ID (ALT 14)
36. The analyst provides the parent node ID (ALT 15)
37. The analyst provides the relationship label
38. The analyst selects the option to accept (ALT 16)
39. The system verifies that the child node and parent node exist (ALT 17)
40. The system creates a Relationship object and stores it in the database
41. The system displays a graphical representation of the newly created relationship between the child node and parent node within the graph of the vector.
42. The system displays the Relationship created in the graph view and table view of the main window
43. The analyst selects the “Export as PNG” option from the Graph right-click drop-down menu
44. The system creates a PNG file of the current vector’s graph and prompts the user to provide a filename and directory in which to save it.
45. End of Use Case

Alternate Paths:

ALT 1: Analyst selects “Connect” option.

ALT 2: Analyst selects “Continue Local” option.

ALT 3: Analyst selects “Exit” option.

ALT 4: System was not able to confirm correct validation parameters or directory structure, warning message will pop up and will not let the analyst continue unless corrected.

ALT 5: System detects image and uses OCR to turn into log files.

ALT 6: System detects audio files and uses audio transcriber to convert to log files.

ALT 7: System doesn’t cleanse the log files.

ALT 8: System doesn’t connect to Splunk.

ALT 9: System doesn’t validate the log files.

ALT 10: The analyst decides to not continue.

ALT 11: The analyst doesn’t select the option to accept

ALT 12: The analyst decides not to hide the nodes

ALT 13: The analyst selects a different option in the right click menu.

ALT 14: The analyst doesn’t provide a child node ID.

ALT 15: The analyst doesn’t provide a parent node ID.

ALT 16: The analyst selects the cancel option.

ALT 17: The system can’t verify the existence of the child and parent node.