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. The analyst

Post-condition: On successful completion the analyst was able to export a graph created and any work done was saved by the system.

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 project, or exit the system.
3. Analyst selects “New Project” option (ALT 1, ALT 2)
4. System displays window comprised of a checkbox to determine if analyst will be the lead for the project and fields to enter event name, event description, event start timestamp, event end timestamp, root directory, red team folder name, white team folder name, blue team folder name, and the lead’s IP address (if the analyst does not choose to be project lead)
5. The analyst decides to be the lead (ALT 3).
6. The analyst decides to not be the lead.
7. 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, and the lead’s IP address.
8. The system cannot verify that there is a direct connection to the lead (ALT 4).
9. The system verifies that there is a direct connection to the lead.
10. The analyst selects the “Ingestion” option (ALT 5, ALT 6).
11. The system saves Event Configuration in the DB.
12. The system connects to Splunk (ALT 7).
13. The system sends all log files to Splunk (ALT 8).
14. Splunk completes processing log files.
15. The system retrieves log entries from Splunk (ALT 9).
16. The system generates a report with errors found it the ingestion process.
17. The system displays a report with the error details (ALT 10).
18. The analyst selects the “force validate” option (ALT 11).
19. The system force validates the files.
20. The system saves the files to the Database.
21. The system displays the main window to the analyst.
22. The analyst selects the option “Add Vector”. (ALT 12)
23. The analyst selects the desired log entries to associate with a selected vector.
24. The system creates the selected log entries into nodes making them significant log entries and visible in the graph.
25. The analyst wants to hide selected nodes in the graph. (ALT 13)
26. The system changes the selected node’s visibility to true and hides the nodes from the graph. (ALT 14)
27. The analyst selects “Add Relationship” option from the Graph drop down menu (ALT 15)
28. The system prompts the analyst to input Child node, Adult Node, and Label Description within the specified field area for New Relationship
29. The analyst enters Child Node, Parent Node, and Label Description input into the associated field area. (ALT 16)
30. The system creates a Relationship object with the analyst’s input
31. The system sends the Relationship object to the Database to be saved
32. The system creates a graphical representation of the newly created relationship between the child node and adult node within the graph of the vector
33. The analyst selects “Export Graph” option from the Main drop-down menu (ALT 17)
34. The analyst selects “PNG” sub option branching out from the “Export Graph” (ALT 18)
35. The system creates a PNG file of the vector’s graph onto the desktop of the analyst’s computer
36. End of Use Case