**Graphical user interface, application

Description automatically generated**

**NCL CTI Report Analyzer Visualization Intern Assignment [07/05/2022]**

**Project Description**

This assignment is a sub project (visualization) of NCL “Towards Automated and Large-scale Cyber Attack Reconstruction with APT Reports” (CTI Report Analyzer) Project. The CTI Report Analyzer is aimed to provide an automated platform for researchers and analysts to expedite their understanding and significantly reduce their turnaround time in addressing cyberthreats.

The current NCL CTI Report Analyzer is a commend line-based system. The developer can do all the configure by cmd and monitor the process by checking the log. The CTI Report Analyzer Visualization will create Application and Web based UI for NCL customers to use and monitor the process to convert the rich details found in CTI reports to reconstruct a dynamic environment. It is a group programming project aims to let National Cybersecurity R&D Laboratory (NCL) interns can pick up the knowledge about CTI report, different kinds of APT events, python UI development and webpage design. Then create an Application and Web which NCL user can use it to control and monitor their CTI report analysis process. The program general design diagram is shown below:

Diagram

Description automatically generated

**Project details**

Project type: Program Visualization, group Intern project

Project workload: 3 day/week, total 12 week.

1. **Assignment Introduction**

**1.1 Assignment background**

National Cybersecurity R&D Lab (NCL) was established in 2015 and funded under the National Cybersecurity R&D (NCR) Programme. NCL is providing support to the Singapore Cybersecurity R&D Community in terms of their R&D, research experimentation and testing requirements. One of NCL business service is providing the provide an automated platform for researchers and analysts to expedite their understanding and significantly reduce their turnaround time in addressing cyberthreats.

Cyber Threat Intelligence (CTI) reports are valuable sources that researchers and analysts seek to have a deeper understanding of the current APT activities and the cyberthreat landscape. These reports are used to obtain insights of vulnerabilities and their associated attack techniques.

The CTI report analyzer UI project is aimed to provide two kinds of user interface which allow NCL customers can directly control and monitor their CTI report analysis progress. The program workflow is shown below:

Diagram

Description automatically generated

The CTI report Analyzer UI contents 7 main modules

1. **CTI Report Analyzer UI App Module**: Application program main frame running on users' local computer to initialize other modules with individual threads.
2. **Data Manger Module**: Data processing module used to handle the input data checking, report file converting and data pre-processing for the CTI report which user upload.
3. **Application User Interface Module**: The main UI module customers used to upload the CTI report, configure the report analysis parameters, monitor report analysis process, and check the result.
4. **Communication Manager Module**: The communication module to handle the data updating and data transfer (such as report upload).
5. **Webpage UI Module**: The Web page with the same function as the Application UI module.
6. **Web Host Module**: The Web Host program to handle the user control on the UI and provide same function as the data manager.
7. **Control Hub Adapter**: The main control hub used to collect data from the CTI report analyzer and the result data base.

In this assignment the Intern are expected to implement the “Application User Interface Module”, “Webpage UI Module”, “Web Host Module”.

**1.2 Related knowledge and reference doc**

The related knowledge needs to learn for the project:

* CTI report.
* Python user interface programming (wxPython)
* HTML, CSS, JavaScript
* Python web host programming (flask)

Needed document:

* NDSS2022Poster\_paper\_37\_final.pdf

1. **Assignment Main Task**

**2.1 Task 1: CTI Report Analyser Application UI.**

This task is aiming create 8 modules to show pop-up window to let the user to control/config their CTI report analysis and monitor the progress.

1. **CTI Report Loader**: The user can use this module to upload the CTI report they want to analyze or select the reports provided by NCL. The module will pre-check the report’s format.
2. **CTI Report Analysis Configure Module:** This module provides the report analysis algorithm selection and show the analysing progress of the current report.
3. **Artifact Description Module**: After the CTI report analysis process finished, the result will show some artifact from the report, this module will provide a description dashboard for use the check the artifact result.
4. **Artifact Reconstruction Config Panel**: The control panel to configure the NCL Artifact reconstruction process.
5. **APT Events Display Dashboard:** A display dashboard panel to show all the APT event tree based on the report analyse result.
6. **Procedure Description**: Under Editing.
7. **Screen Play**: Open browser to show the related NCL analysis/demo onine video.
8. **Testbed Configuration Module**: Using both Screenplay and related artifacts, an environment is reconstructed on the testbed. The reconstructed environment simulates the APT attack that is described in the CTI reports. Such simulated environment allows analysts to dynamically understand the APT attack. User can use this module to config the testbed and monitor the testbed working statues.

Expected workload: 3 day/week, total 12 weeks.

**2.2 Task 2: CTI Report Analyser Web UI.**

[Optional] The Intern will develop the web interface with the same function as the task 2.1

Expected workload: 3 day/week, total 12 weeks.

**2.3 Assignment Final Goal**

After finished the assignment, the Intern students need to provide below document and program:

1. Provide an Intern assignment proposal/timeline plan.
2. Provide at least 4 workable modules of CTI Report Analyser Application UI.
3. [Optional] Provide the CTI Report Analyser Web UI and the webhost program.
4. [Optional] Provide a knowledge sharing doc to share with other interns about the learning experience.

The Intern need to finish and submit all these files for project evaluation:

1. Improved assignment introduction doc: CTI Report Analyzer Application UI \_Intern.docx
2. Project progress tracking doc: TimeLine.md
3. Intern project final report: CTI Report Analyser Application UI \_final\_report.doc
4. Intern project final presentation: CTI Report Analyser Application UI \_final\_report.pptx
5. Project problem and solution tracking document: Problem and Solution.docx
6. **Assignment Timeline/Milestone**

Below is the project timeline draft and we will do adjustment and change in the future. We may do a very short discussion every week and every month to track the project progress.

|  |  |
| --- | --- |
| **Week Index** | **Task/Milestone** |
| Week 1 | * Improve the project design document. * Create a project implement plan timeline document. (TimeLine.md) * List down all the knowledge need to pick up. |
| Week 2 | * Pick up the related API and programming knowledge. * Create some simple test program during leaning. |
| Week 3 | * Start testing and continues knowledge learning if needed. * Setup the main program on local computer. |
| Week 4-7 | * Program development for main features. |
| Week 8-9 | * Program improvement and add new features. |
| Week 10-12 | * Finish all the documents. * Short presentation to the team. |

1. **Reference**

The Intern can list down all the links/document he used for the project here:

NDSS2022Poster\_paper\_37\_final.pdf