



Ransomware Anomaly Detection

Student: Bryan Simmons

Mentors: Mike East, Kaseya; Carl Banzhof, RocketCyber

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

PROBLEM

With Ransomware being the fastest growing type of cyber crime in the world, the need for more advanced software capable of detecting ransomware has become increasingly important. This project was focused on using Machine Learning find anomalies within Windows logs to find signs of Ransomware.

CURRENT SYSTEM

Python-based application that reads .evtx Sysmon archive files, parses them to get event data, and passes that data to an algorithm that determines the event dissimilarity compared to previous events.

REQUIREMENTS

Hardware:
Requires a machine with at least 10 Windows OS.

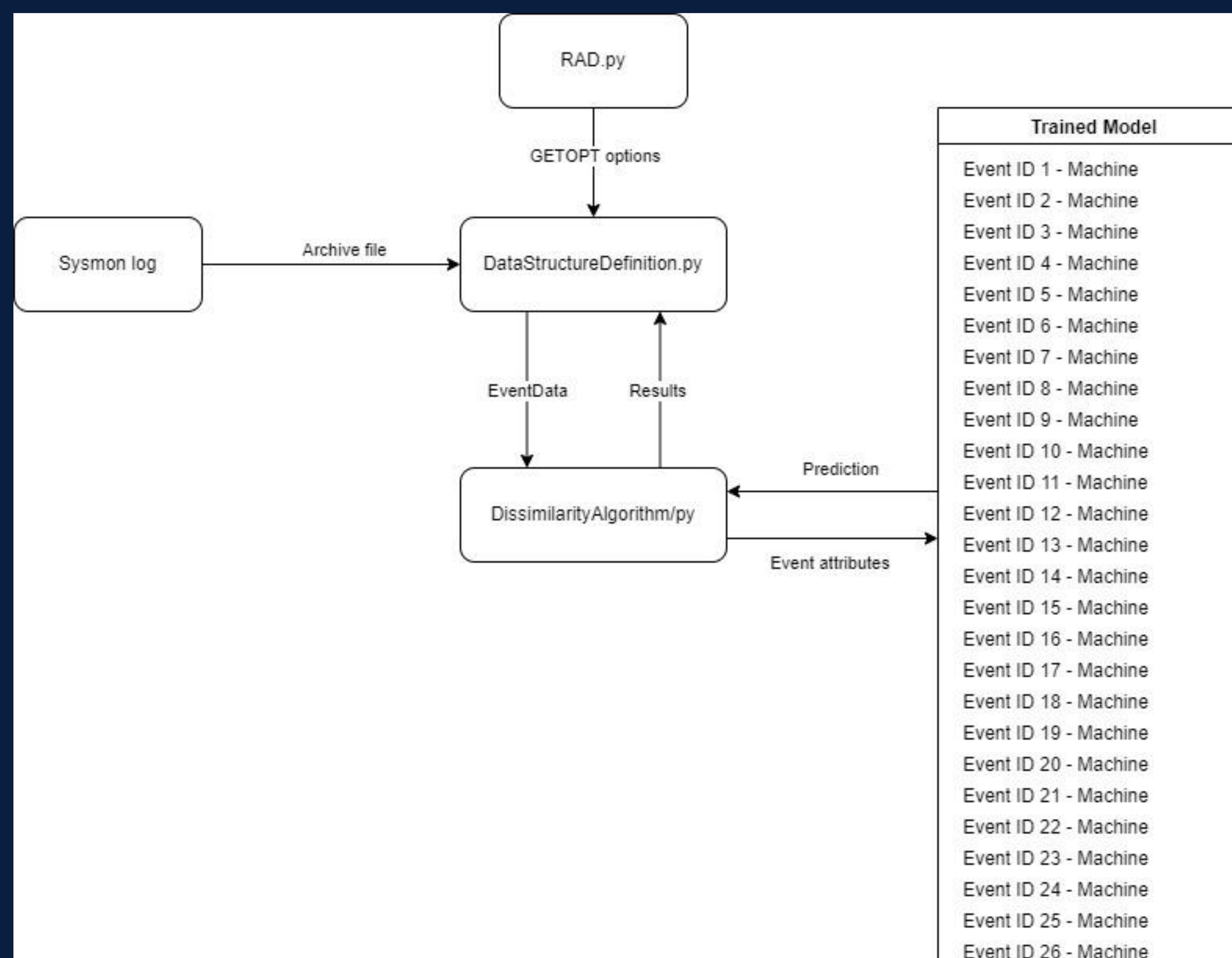
Software:
Windows Sysmon logging tool.
Python 3.10.
Visual Studio Code.
GitHub versioning system.
Sysmon Simulator used for testing

VERIFICATION

Application was tested using the Sysmon Simulator application that mimics ransomware events in the Sysmon log files.

Application found the anomalies with a success rate of 75%, with less than 1% of the sample being false positives

SYSTEM DESIGN



SUMMARY

I was responsible for:

- Machine Learning algorithm (using a Ratcliff-Obershelp string comparison function)
- Command-line interface (GETOPT)
- Model structure (k-means clustering)
- Sysmon Simulator testing

REFERENCES

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

<https://github.com/ScarredMonk/SysmonSimulator>

USAGE

Program usage:

```
-i (input path) -> use provided log location instead of default
-p              -> return a prediction of the events analyzed
-s              -> Do not delete log files after analyzing them
-f (input file) -> Only analyze the file given
-a              -> Analyze all logs files in the target folder (not recommended)
```

If program is not run as admin it will request admin rights and run in a new window

ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by XXXXX (name of the project sponsor: federal, state or local government, or corporate partners, where applicable). We/I thank XXXX for his/her/their assistance and mentorship that I/we received throughout the senior design project.

