

Ransomware Anomaly Detection

Students: Sebastian Duenas

Mentor: Mike East, Kaseya; Carl Banzhof, RocketCyber

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

PROBLEM

Ransomware network attacks have become an increasingly important threat in the last 28 years and government integrated systems in the last 10 years.

This project is focused on using Machine Learning in order find anomalies within Windows logs and locate suspicions of Ransomware.

CURRENT SYSTEM

The three different ransomware attack techniques are signature-based detection, behavior-based detection, and deception-based detection

Our project is a Python application that reads .evtx archive files generated by the Sysmon application. Once the application parses the Sysmon logs to get event data, that data is passed to the algorithm. The algorithm then determines if the event dissimilarity compares to previous normal events.

SUMMARY

We were able to develop an initial functioning anomaly detection that can predict abnormal behavior using Sysmon Windows event logs. I was tasked with researching the implementation of Sysmon and Windows Event log data, the implementation of Machine Learning and completion of 5 of the user stories

IMPLEMENTATION

Machine Model:

- Dissimilarity String Comparison

Hardware:

- At least Windows 10 operating system

Software:

- Windows Sysmon logging tool.
- Python 3.10.

REQUIREMENTS

It included the research and local testing of machine learning algorithms, different approaches, and tools. As well as Sysmon application for creating logs Python runtime environment Sysmon Simulator used for testing

VERIFICATION

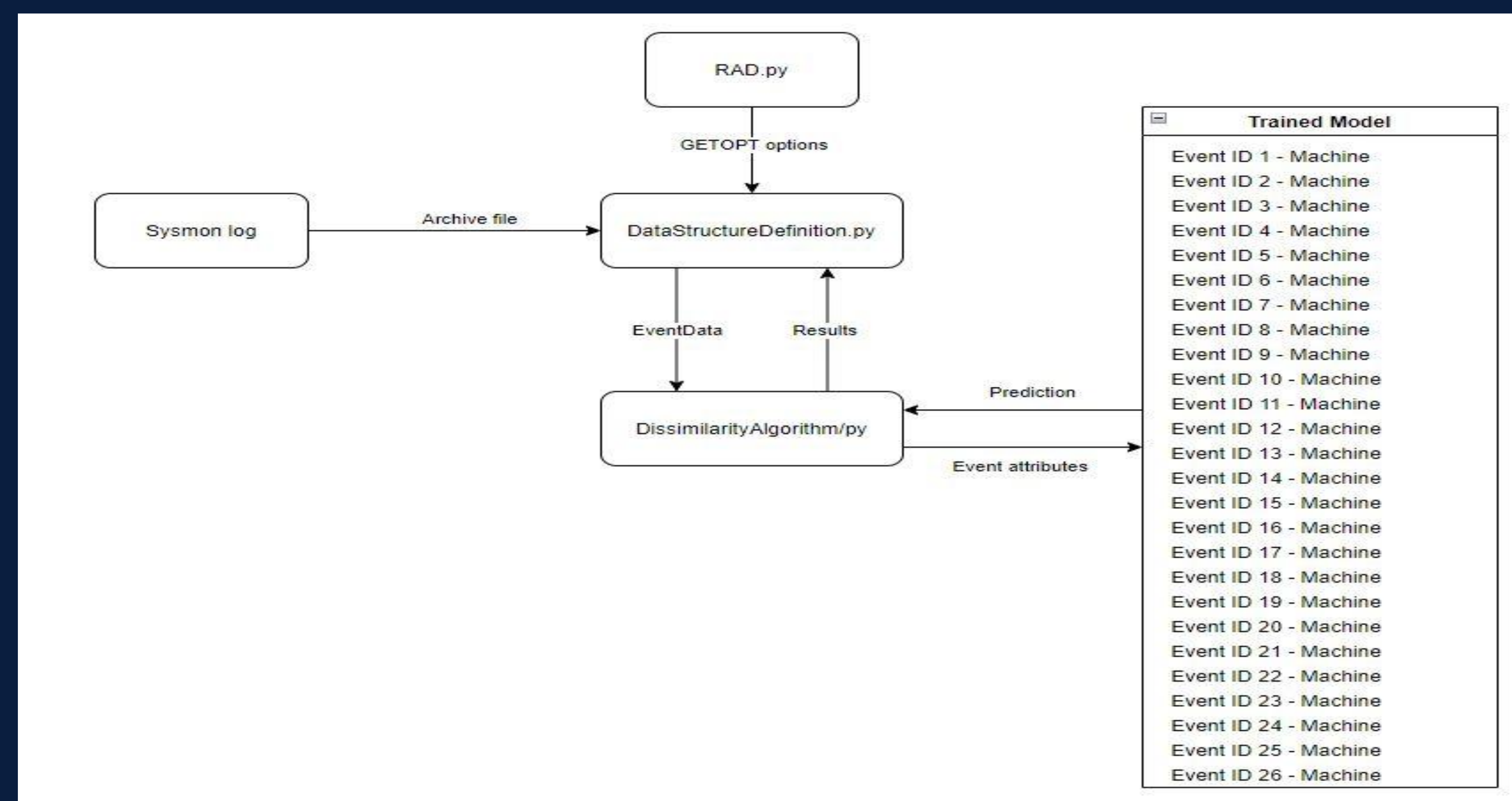
This application was tested and verified using the Sysmon Simulator application which mimics ransomware events in the Sysmon v13.33 log files

REFERENCES

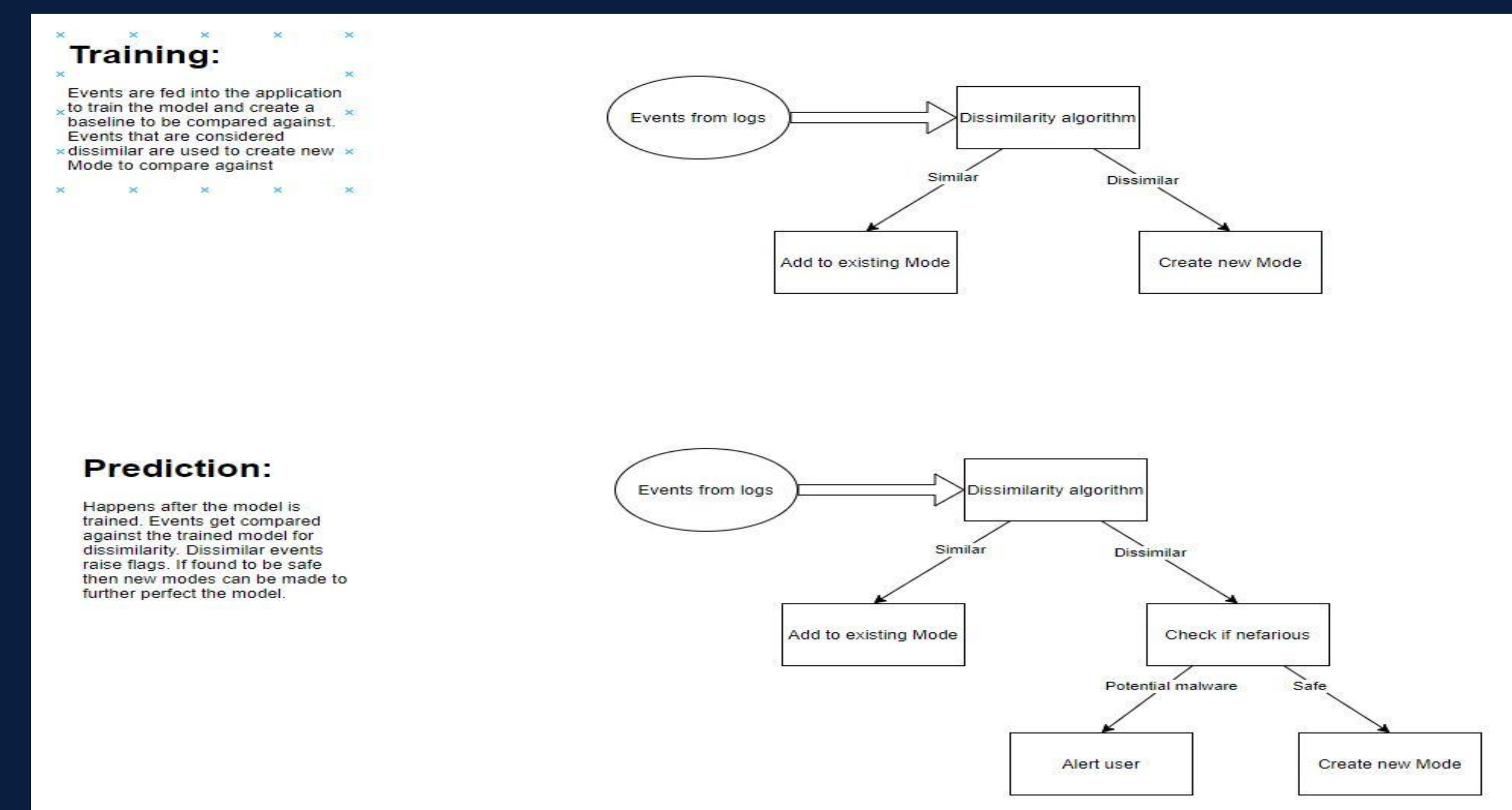
<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

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

SYSTEM DESIGN



OBJECT DESIGN



ACKNOWLEDGEMENT

We thank Professor Masoud Sadjadi, and Mike East and for their assistance and mentorship that we received throughout the capstone 2 design project.