



Knight Foundation
School of Computing
and Information Sciences

Knight Foundation School of Computing & Information Sciences

Spring 2022 Senior Design Project

Ransomware Anomaly Detection

Student: Yaohua Hu

Mentors: *Mike East, Kaseya; Carl Banzhof, RocketCyber*

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

PROBLEM

New cybersecurity threats emerge frequently. One such threat is ransomware, which saw an increase in strength and frequency in the last 28 years since its creation. Today, a multitude of ransomware variants exist that disrupt personal computers, network servers, and critical economic infrastructure.

On May 7, 2021 Colonial Pipeline Co. , an American oil pipeline system company, was attacked by ransomware from a hacker group called DarkSide. It breached the IT network through a virtual private network account. The hackers threatened to steal nearly 100 gigabytes of data from Colonial Pipeline Co. and then they would leak the data if the ransom was not paid. Colonial Pipeline Co. paid the ransom of a \$4.4 million shortly after the hack while in the meantime, led to Colonial's temporary shutdown that halted roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard which disrupted the oil supply chain of the U.S economy. [1] [2]

The focus of this project is to develop a machine learning (ML) algorithm that will predict accurately the detection of ransomware through analyzing metadata from Sysmon application event logs which is classified as anomalies

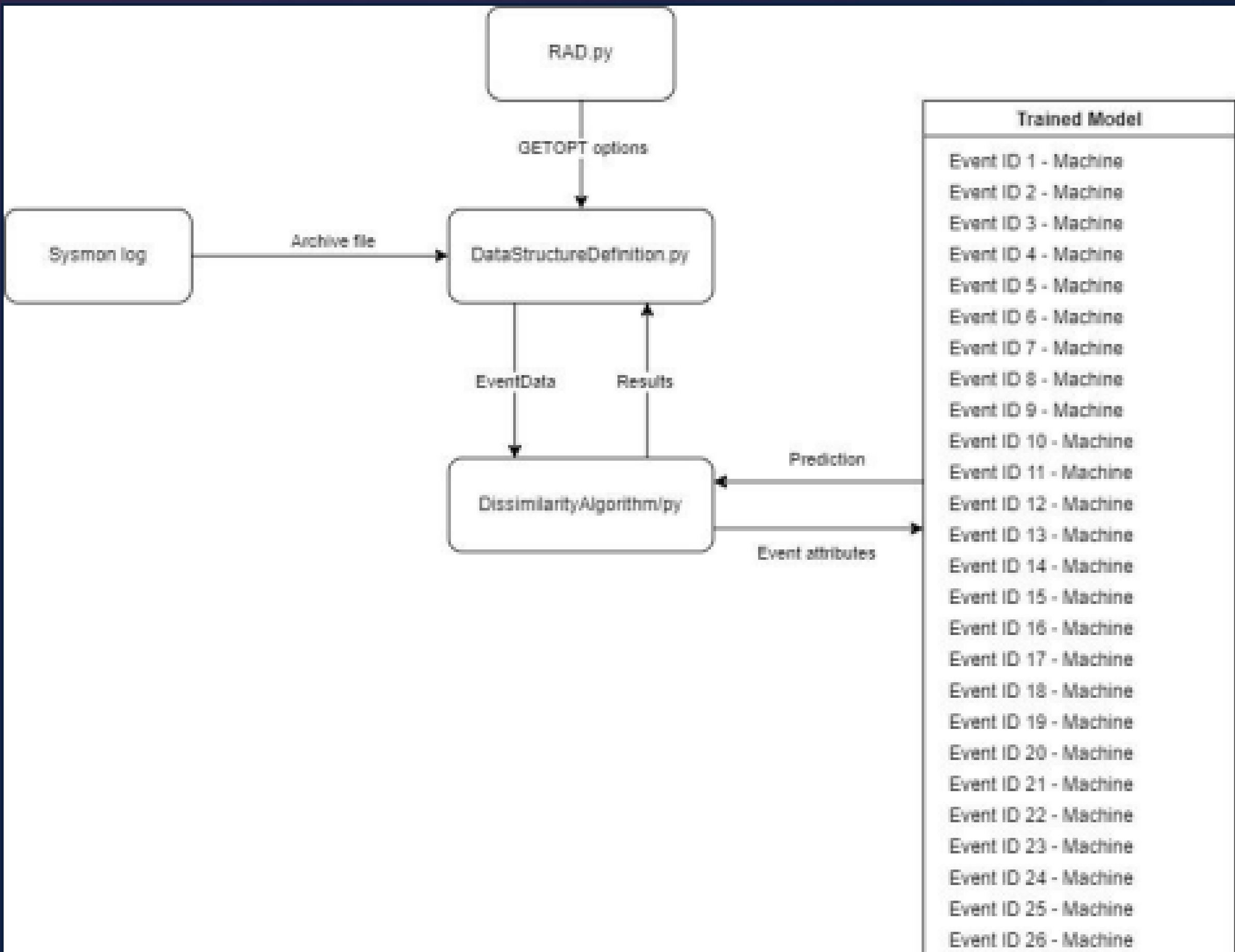
CURRENT SYSTEM

There are many red flags that reflect an occurrence of a ransomware attack. These behavioral patterns in computer systems are recorded as event log files (.evtx) which can help us depict the occurrence of a ransomware attack. The listed actions can be used as a flag for the ML agent to detect the launch of a ransomware attack.

- (1) Opening of many files
- (2) Structure of input and output streams to a process is different
- (3) Many write/overwrite operations
- (4) A process calling encryption APIs
- (5) Frequent reading and rewriting/deleting requests in a short period of time
- (6) Communication with command-and-control server
- (7) Change in the user registry keys

The current system of our project is a Python application that reads .evtx archive files generated by the Sysmon application, the application parses the Sysmon logs to get event data and passes that data to our modified nominal attribute matrix algorithm that determines the event dissimilarity compared to previous normal events.

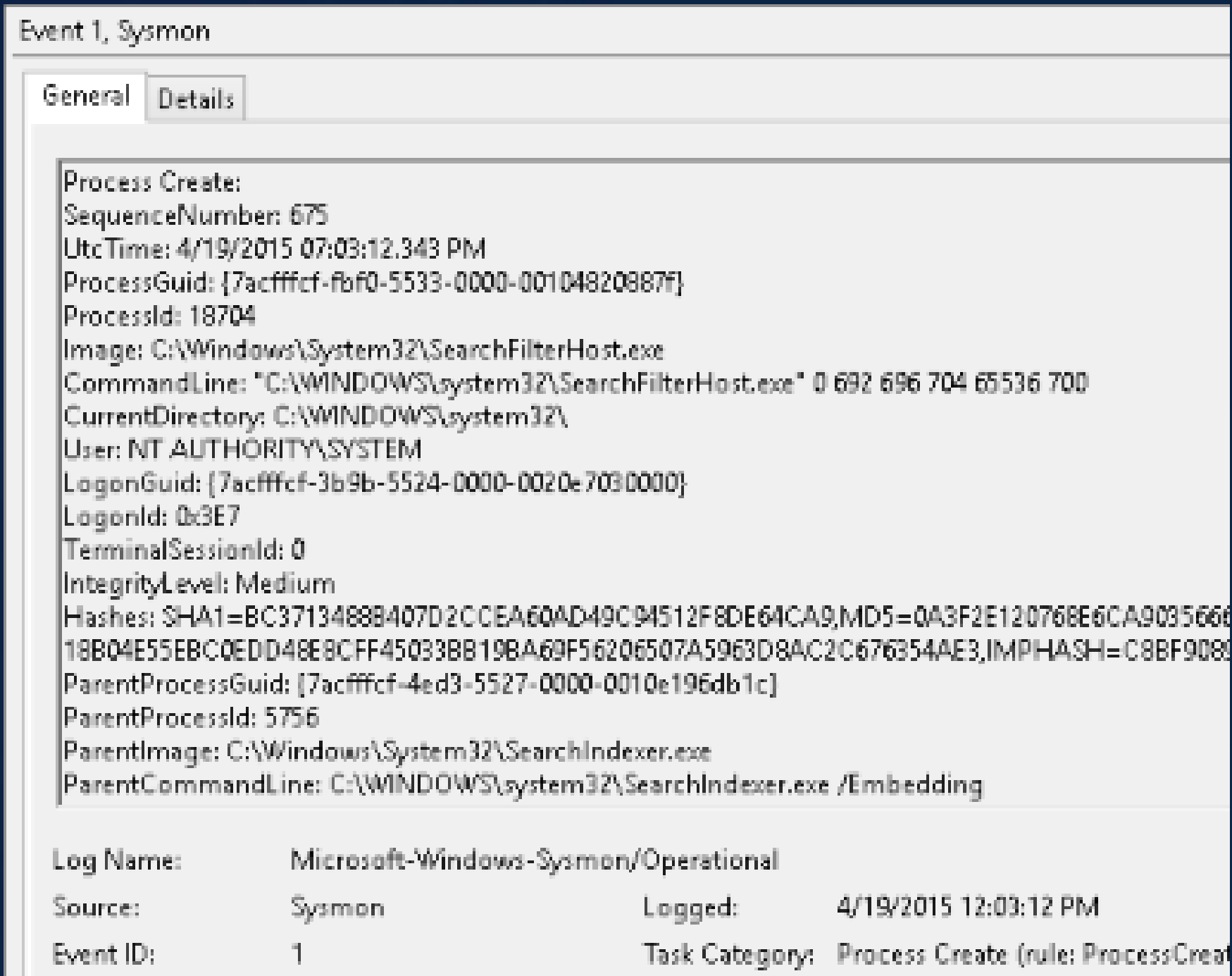
SYSTEM DESIGN



IMPLEMENTATION

The learning machine model used our Dissimilarity String Comparison algorithm that was support by a nominal attribute matrix for the twenty-six Sysmon Event IDs.

- Software:
- The project requires a Windows 10 operating system environment
 - Python 3 runtime environment: The main programming language used to create our project (Ransomware Anomaly Detection)
 - Scarred Monk's Sysmon Simulator: Necessary tool needed to test a simulated ransomware attack for create our project (Ransomware Anomaly Detection)



Screenshot of event log metadata information used for our project from Microsoft Windows' Sysmon v13.33 application [3]

SUMMARY

The main project contributions I did were:

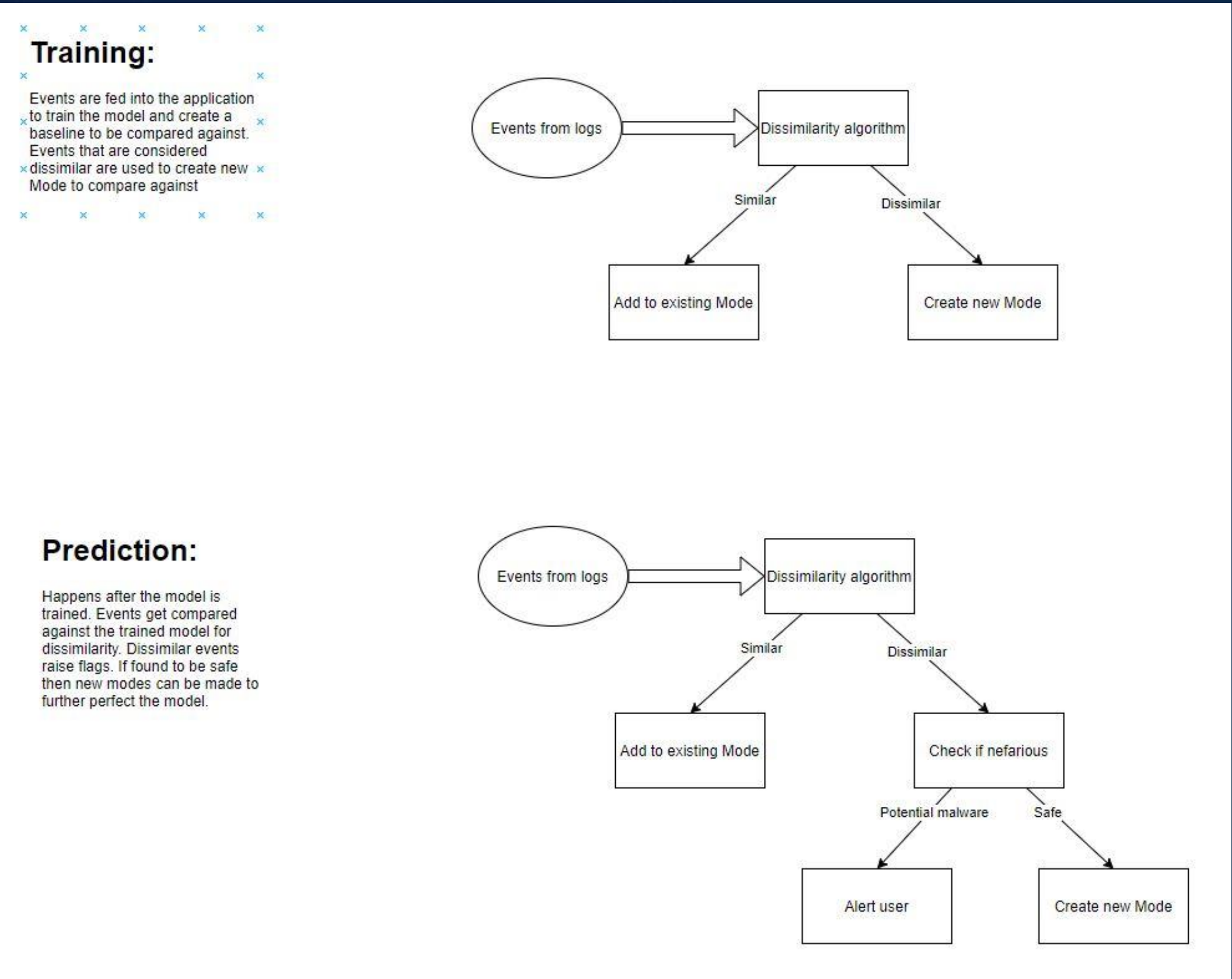
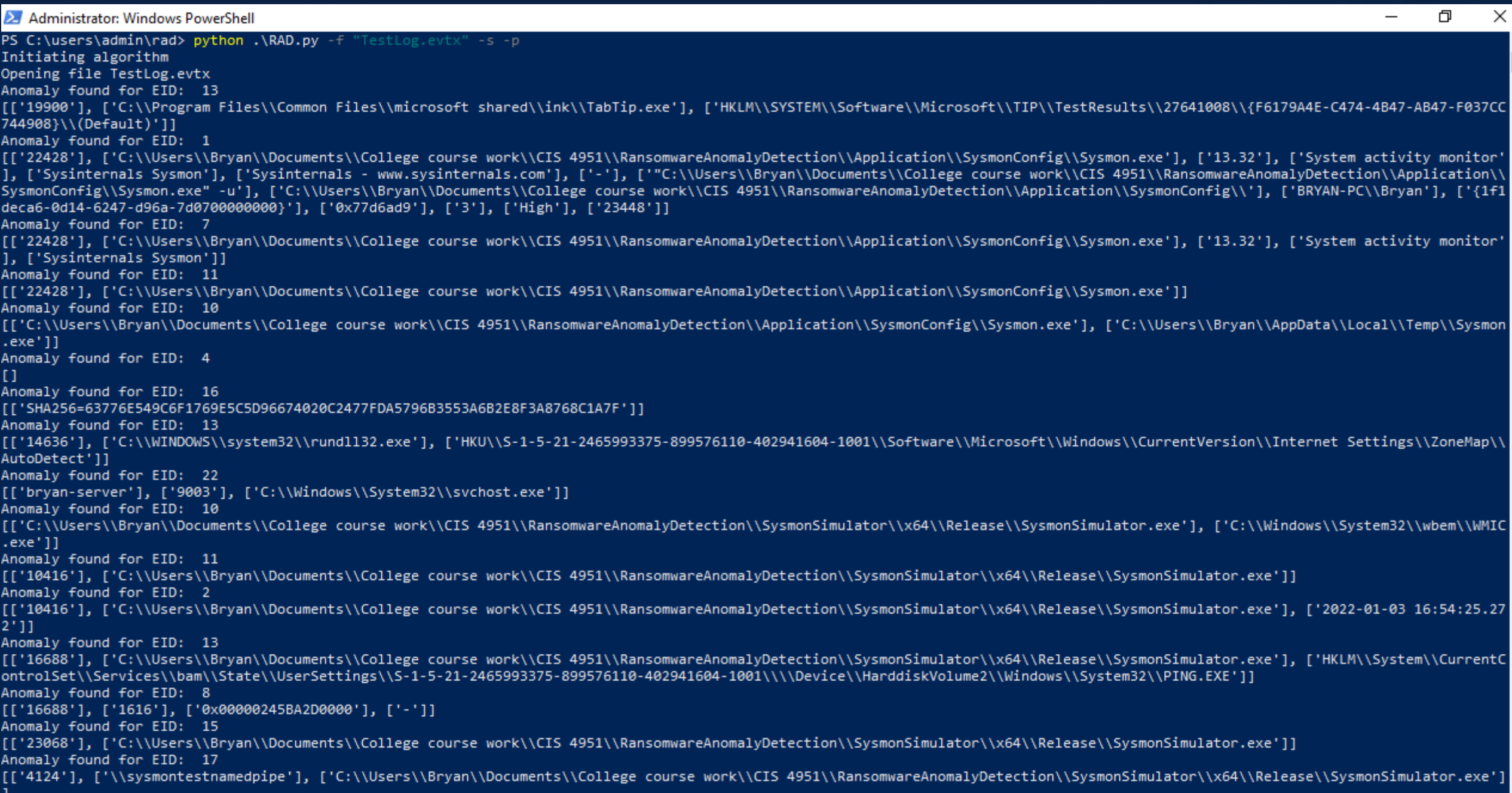
- Researched and partial Implementation of Sysmon and Windows Event log data parsing through win32evtlog Python module
- Researched and tested various Machine Learning anomaly detection algorithm(s) that could function with the Ransomware Anomaly Detection project such as LocalOutlierFactor, K-Means Clustering, and K-NN that helped lead to develop our Dissimilarity String Comparison algorithm
- Partial implementation of object serialization in Python for our learning machine model
- Researched and assisted in development of Event ID nominal attribute matrix to support the Dissimilarity String Comparison algorithm
- Support other team members with other User Stories
- Research and test various data visualization models using Python's matplotlib library

REFERENCES

- [1] Colonial Pipeline Cyber Incident. Energy.gov. (n.d.). Retrieved April 17, 2022, from <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>
- [2] Turton, W., & Mehrotra, K. (2021, June 4). Bloomberg.com. Retrieved April 17, 2022, from <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
- [3] Russinovich, M., & Garnier, T. (2022, February 16). Sysmon - Windows Sysinternals. Sysmon - Windows Sysinternals | Microsoft Docs. Retrieved April 17, 2022, from <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
- [4] Monk, S. (2022, January 7). Understanding sysmon events using SysmonSimulator. RootDSE. Retrieved April 17, 2022, from <https://rootdse.org/posts/understanding-sysmon-events/>

VERIFICATION

Our application was tested using the Sysmon Simulator application that mimics ransomware events in the Sysmon v13.33 event log files.



Engineering
& Computing

The material presented in this poster is based upon the work supported by *Carl Banzhoff*. I thank *Carl Banzhof and Mike East* for their assistance and mentorship that we received throughout the senior design project.