In order to deal with an attack on a network, the attack must first be detected. Therefore, we need to place sensors around our network to collect data that could signal a potential attack.

However, how do we know where to place the sensors to maximize detection? Additionally, is the data we are collecting even relevant and accurate? If we collect all data, the chance for false positives increases.

The measurement of how a network’s monitoring strategies effectively address the above issues is called observability. In order to calculate observability, James Halvorsen, Jesse Waite, and Adam Hahn developed a tool called TOMATO.

They already conducted research into the effectiveness of TOMATO, so our project is an extension of their previous work.

We use a new SIEM/data aggregation tool called Wazuh which aggregates data from Suricata, Sysmon, and Windows Event Channels.

The previous experiment used the ELK Stack (Elasticsearch, Logstash, and Kibana) to aggregate data from Sysmon, Windows Logs, and Netflows.

As a result, our project seeks to test TOMATO on measuring the observability of more SIEM/data aggregation tools.

We are also looking into the possibility of expanding the previous experiment by using new tactics.

### MITRE ATT&CK FRAMEWORK

A database of tactics and techniques that adversaries use against computer systems. It’s maintained by the MITRE corporation.

It was developed by the MITRE corporation.

### EXPERIMENTAL SETUP

Our experiment consists of five computers. Four are Windows 10 machines that generate network traffic between each other. The fifth is an Ubuntu Linux machine that hosts the Wazuh server.

On all of the Windows 10 Machines, we use Wazuh agents to collect data from Sysmon, Windows Event Channels, and Suricata.

This information gets stored in the Wazuh server and can be processed using the ELK Stack.

Sysmon: A Windows system service that collects system information and logs it in the Windows Event Log. We use it to log process creation events.

Windows Event Channels: These channels store information about events that correspond to applications, security, and the system of a windows machine.

Suricata: A network intrusion detection system that stores information on network events into and out of a host.

### REFERENCES


### ACKNOWLEDGEMENTS AND FUNDING

The authors are grateful for funding from the Griffiss Institute under contract No. SA10012021MM0336.