Problem Statement and Goals

In Jan. 2018, a NIST draft to the Cybersecurity Framework called for the development of cyber security metrics, saying such work would be a “major advancement and contribution to the cybersecurity community.” This research seeks to do just that by developing metrics based on the CIS Critical Security Controls. Along with this contribution, a proof of concept is implemented for two of the metrics.

Approach

CSC #8: Malware Defenses has a total of six sub controls aimed at controlling the “installation, spread, and execution of malicious code.” The majority of metrics developed focus on quantifying the desired behavior as an overall percentage of all behavior captured. Metric derived from data fusion of security logs, have the potential to increase situation awareness to strategic decision makers, & systems administrators. Metrics are built for each of the sub controls for CSC 8.

Results

Along with the development of these metrics, a proof of concept is implemented in a computer network designed to mimic a small business that is using Symantec Endpoint Protection and Splunk. A Splunk dashboard is created to monitor, in real time, the status of CSC 8.1 and 8.2. Each dashboard featured measurement banners that provide quick access to top level metrics. A fused data table provided actionable information for future investigation by a systems administrator.

In the future, my colleagues and I will pursue the development of metrics for each of the Critical Security Controls.