ABSTRACT

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. (National Institute of Standards and Technology, 2017b)" Unfortunately, defining security and the role of metrics in compliance continues to be a place of disagreement. Along with this, research around measuring security fails to present detailed guides on how to implement security metrics collection and reporting.

This research seeks to explore how measuring Critical Security Controls, through data fusion of security logs, helps increase situation awareness to strategic decision makers, and systems administrators. Metrics are built for each of the sub controls for Critical Security Control 8: Malware Defenses. Along with the development of these metrics, a proof of concept is implemented. This implementation highlights some of the benefits found through a metrics program in an organization. This work contributes to the industry's need for cyber security metrics while providing a detailed implementation guide to those security practitioners looking to implement metrics in an organization.