

SYSTEM AND METHOD FOR HIGH SPEED THREAT INTELLIGENCE MANAGEMENT USING UNSUPERVISED MACHINE LEARNING AND PRIORITIZATION ALGORITHMS

ABSTRACT

This document discloses a system and method for consolidating threat intelligence data for a computer and its related networks. Massive volumes of raw threat intelligence data are collected from a plurality of sources and are partitioned into a common format for cluster analysis whereby the clustering of the data is done using unsupervised machine learning algorithms. The resulting organized threat intelligence data subsequently undergoes a weighted asset based threat severity level correlation process. All the intermediary network vulnerabilities of a particular computer network are utilized as the critical consolidation parameters of this process. The final processed intelligence data gathered through this high speed automated process is then formatted into predefined formats prior to transmission to third parties.

FIGURE 1