Questions 04-02-2018

Intrusion detection and big heterogeneous data: a survey:

This article discusses heterogeneity of big data in cyber security. One of the ideas presented is that analyzing data from heterogenous sources with a great deal of variety can lead to better cyber security. Do we think security information and even management systems are a good way to do this? What tools do we think a good SIEM would use to accomplish this goal?

Big data based security analytics for protecting virtualized infrastructures in cloud computing:

A big-data based security analytics approach involving graph-based even correlation, map-reduce parsing, and two forms of machine learning is presented in this article. The results of this proposal are explained as it is compared to other similar approaches previously researched. One of the previous approaches that is much faster, on average, than the proposed approach is Livewire. Livewire is much faster due to being deployed in each VM instead of the proposed approach which communicates overs ssh. Can we think of instances where one or the other may be more useful? Do they have their niches, or is one universally better?