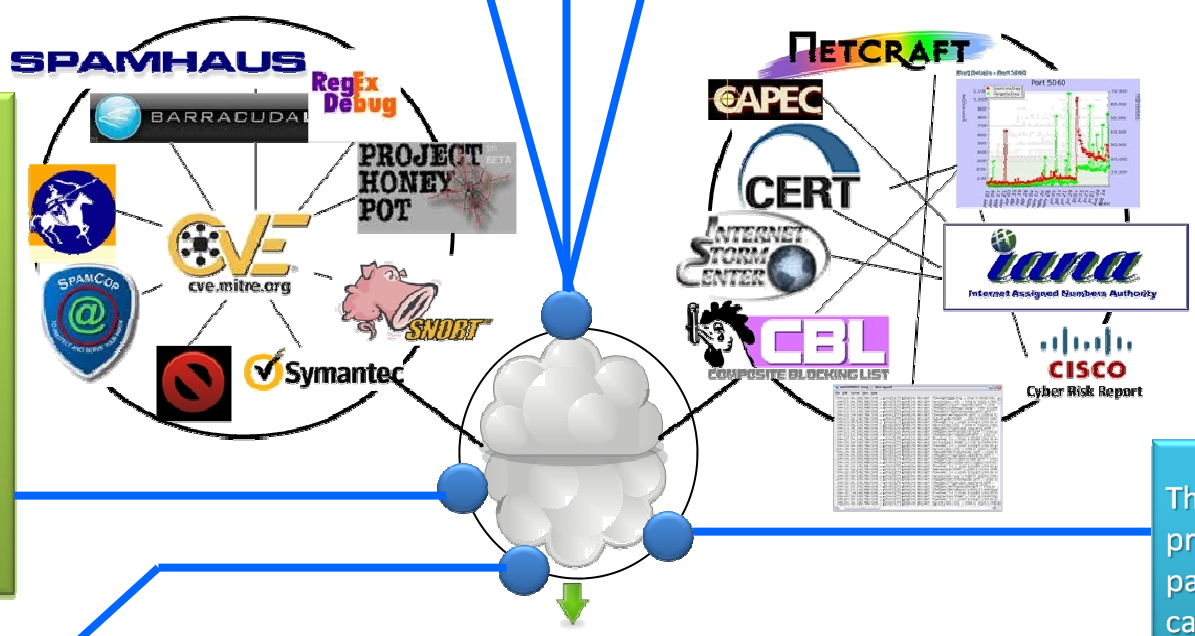
The 6th International Conference on Software and Data Technologies 2011 | Spain | 18-21 July 2011 ICSOFT 2011

Research on Heterogeneous Data for Recognizing Threat

Large of volume network security signature and multidimensional data has grown rapidly in recent years.

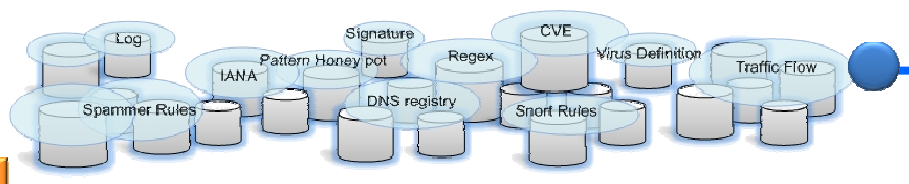
The ability to extract hidden pattern and trends from large quantities of ***heterogeneous data*** is important for immune & predict before attack

In this study, Data Mining is used to perform data collection using history, patterns, and relationships between classification and estimation of attack in stream network.



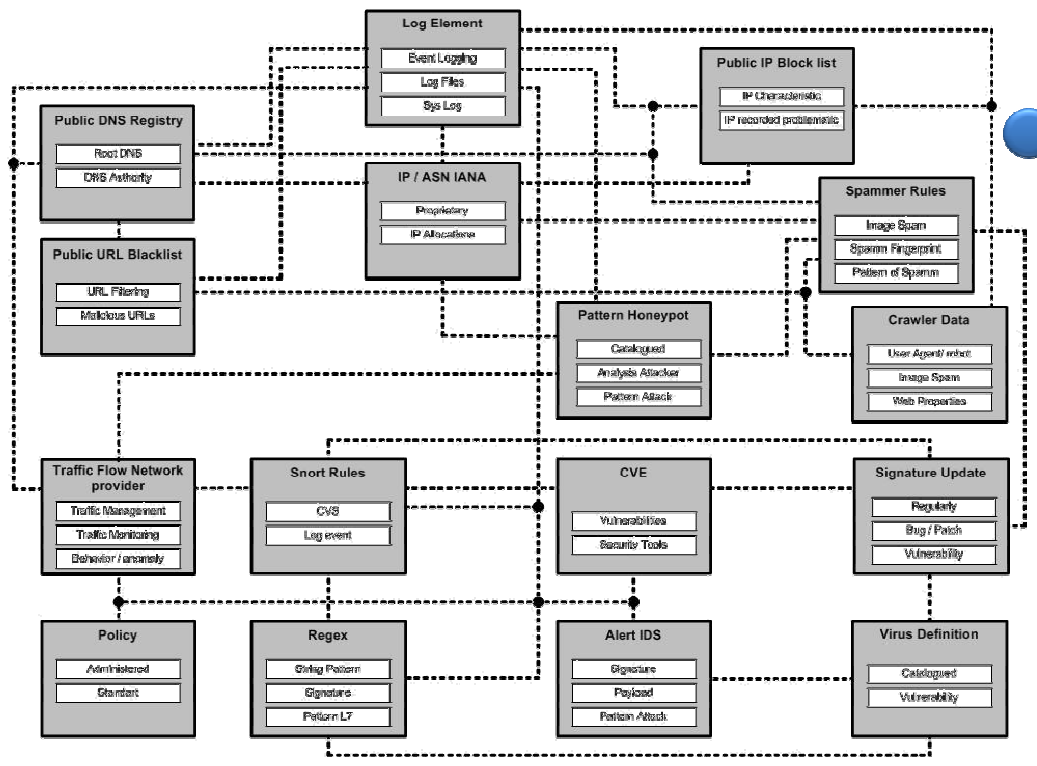
These heterogeneous data includes signature identification, rules, policy, pattern, method attack, URL blacklist, update patch, log system, list of virus variance and regular expression, all these will be collected and labeled to identify attack patterns and can be predicted that it would occur.

There are opportunity to make prediction future threat from past experiences, these scenario called text categorization, making a prediction requires more that a lookup of past experience



Critical need of data analysis system that can automatically analyse the data to organise it and predict pattern attack future trends.

Learning technique from Data Mining can be solution for research objectives (i) prediction of attack pattern, (ii) identification from anomaly habitual activity, (iii) estimation normal activity based on habitual activity, (iv) classification attack / suspicious packet, (v) mapping habitual-activity, and (vi) early prevention of security violation.



We propose to collecting scattered information in routine update regularly from provider or security community. This data can be useful information to be associated with other.

In this work, we showed a data mining approach to collecting scattered information in routine update regularly from provider or security community. This paper addresses problems and existing theories in possible future research in this field.

Faculty Computer Science & Information System, University Teknologi Malaysia

Deris Stiawan
deris@unsri.ac.id

Prof. Dr. Abdul Hanan Abdullah
hanan@utm.my

Dr. Mohd. Yazid Idris
yazid@utm.my