INTISARI

PROYEK AKHIR

ANALISIS TAKSONOMI INSIDEN PADA MISP MENGGUNAKAN PENDEKATAN PENILAIAN ANCAMAN KUANTITATIF

Abstrak - Sebuah instansi atau organisasi harus bisa memprioritaskan ancaman siber mana yang sebaiknya direspons dan ancaman siber mana yang setelah dipertimbangkan ternyata dapat dikesampingkan atau diabaikan. Salah satu caranya adalah dengan menilai dari tingkat keparahan insiden siber yang terjadi. Proses penilaian dapat memanfaatkan taksonomi insiden tersebut. Informasi taksonomi dapat diperoleh dari mana saja salah satunya adalah MISP. Namun, informasi taksonomi haruslah berupa nilai numerik agar dapat dikalkulasikan. Maka dari itu, perlu analisis dan pengolahan data taksonomi. Dengan mengadaptasi metode penilaian ancaman yang sudah ada, penelitian ini akan mengolah data taksonomi sehingga menghasilkan nilai numerik yang dapat merepresentasikan tingkat keparahan dari setiap taksonomi dalam bentuk angka. Nilai numerik kemudian dapat digunakan untuk menghitung tingkat keparahan suatu insiden yang menggunakan data taksonomi sebagai parameter perhitungan.

Kata Kunci: Taksonomi Insiden, MISP, Penilaian Ancaman

ABSTRACT

Incident Taxonomy Analysis on MISP Using a Quantitative Threat Assessment Approach

Abstract - To respond to incidents more efficiently, an organization should prioritize which incidents require immediate response and which incidents may be delayed or ignored for some reason. One of the methods that can be used is to recognize the severity level of the incident. Incident taxonomy can be used to determine the incident's severity level. There are so many sources to get incident taxonomy. One of the most widely used sources is MISP. However, to do the calculation, the taxonomy needs to have a numerical value. In order to give the taxonomy a numerical value, an analysis process is needed. Using an existing threat assessment method, this research will analyze and process incident taxonomies to obtain the appropriate numerical value representing the severity level of each taxonomy in numerical form. The numerical value then can be used as a parameter to calculate the severity level of the cyber incident.

***Keywords**: Incident Taxonomy, MISP, Threat Assessment*