Integrasi Machine Learning dan Analisisnya untuk menghasilkan Snort Rule pada Proyek Mata Elang = Analysis and Integration of Machine Learning to Produce Snort Rules in Mata Elang Project

Yovan Yudhistira Widyananto, author

Abstrak

Keamanan privasi data dan informasi dalam internet sering menjadi topik pembahasan dari waktu ke waktu, hal ini dikarenakan metode penyerangan siber selalu berevolusi menyesuaikan dengan struktur keamanan yang ada, menjadikan bidang keamanan siber menjadi bagaikan kompetisi untuk selalu lebih dahulu dari lawannya. Salah satu contoh implementasi keamanan siber merupakan Intrusion Detection System, dikenal juga dengan IDS. IDS dapat membantu menjaga sebuah jaringan dengan mendeteksi jika ada tanda-tanda penyerangan, namun dengan ini saja tidak cukup untuk memaksimalkan keamanan sebuah jaringan. Dari dasar IDS ini, sebuah proyek mencoba mengembangkan konsepnya dan membuat struktur besar, dan berhasil diciptakan proyek Mata Elang. Struktur Mata Elang dapat menjadi perantara antara internet dengan jaringan yang dilindunginya, dan ketika terjadi serangan, aktivitas tersebut akan dideteksi, ditahan, dan diproses oleh Mata Elang. Sistem deteksi Mata Elang bergantung kepada framework Snort. Sayangnya, Snort tidak memiliki kemampuan untuk beradaptasi di luar dari konfigurasi yang telah diberikan kepadanya. Dalam penelitian ini, penulis akan mengimplementasikan Machine Learning untuk meningkatkan keamanan yang diberikan pada proyek Mata Elang, spesifiknya pada sensornya yang menggunakan Snort. Setelah segala proses perancangan, pembuatan, dan pengujian telah dilakukan, hasil akhir yang didapatkan dari sistem Machine Learning merupakan sistem prediksi yang memuaskan untuk memprediksi kategori serangan bahkan dengan dukungan data yang lemah, namun kemampuan dari aturan Snort yang dihasilkan masih belum diuji dengan matang.

.....

The talk about the security of private data and information will continue to be a relevant topic because of the nature of the concept. Cyberattacks have always been adapting according to the technology and structure that exists at the time, and so cybersecurity will continue to be a competition for gaining the advantage against their contrarian. One of the prime examples in cybersecurity implementation is Intrustion Detection Systems, also known as the shortened term, IDS. IDS can help guard a network by detecting different kinds of anomalies or attacks, although this alone wouldn’t be enough to maximize the level of proper security necessary for a whole network. Under the basic concept of IDS, a project attempts to develop an IDS and create a larger structure. The project was successfully implemented and now titled as Mata Elang. Mata Elang’s structure is an intermediary between an internet connection and the network it is connected to, and when an attack happens, those activities will be detected, interrupted, and then processed by Mata Elang. Mata Elang’s detection system completely relies on the framework Snort. Unfortunately, Snort does not have the capabilities to adapt outside the configurations that has been given to it. In this research, the writer will implement Machine Learning to further increase the security provided by Mata Elang, specifically on the sensors that uses Snort. After every step of the planning, making, and testing has been done the final result of the product was a Machine Learning system that has a satisfactory performance in categorizing the attacks, even with a weak supporting data, however the performance of the snort rules generated by it has

not been tested thoroughly.