Perbandingan kinerja security analytic tools untuk mengatasi advanced persistent threat = Performance comparison of security analytic tools to overcome advanced persistent threat / Amalia Ayu Pratiwi

Amalia Ayu Pratiwi, author

Abstrak

ABSTRAK
Advanced Persistent Threat APT merupakan salah satu serangan yang sulit dideteksi pada saat ini. Tidak ada satupun perangkat yang memberi satu solusi yang dapat mendeteksi ataupun mengatasinya. Dalam hal ini diperlukannya satu solusi yang komprehensif untuk mengatasi serangan tersebut. Pada perbandingan kinerja security analytic tools kali ini, akan diketahui kinerja perangkat tersebut dalam mengatasi APT. Perangkat yang digunakan adalah beberapa perangkat security analytic yaitu Deep Discovery Inspector Trend Micro TM DDI dan Security Analytic Blue Coat SA . Parameter yang digunakan untuk percobaan dalam skenario berupa beberapa jenis malware yang disebar melalui free file sharing dalam bentuk suatu link URL, kemudian link URL tersebut akan diunduh oleh target. Setiap perangkat security analytic diharapkan mengenali ancaman tersebut, sehingga didapatkan tingkat deteksi kinerja perangkat security analytic. Semakin besar nilainya maka semakin baik kinerja perangkat tersebut. Pada tiap perangkat security analytic dapat mengetahui karakteristik serangan dan mampu mengenali tingkatan dampak serangan tersebut. Hasilnya didapatkan bahwa kinerja SA BlueCoat lebih baik dalam mendeteksi ancaman daripada Trend Micro Deep Discovery Inspector TM DDI . Trend Micro Deep Discovery Inspector TM DDI mampu mengenali karakteristik ancaman lebih detail daripada SA BlueCoat.
<hr />
ABSTRACT
An Advanced Persistent Threat APT attack is an attack that is currently difficult to detect. No devices that can detect or resolve it. In this case, there is a need for a comprehensive solution to address such attacks. In this work we perform the comparison of performance of the security analytics tools, i.e Trend Micro Deep Discovery Inspector DDI and Security Analytic BlueCoat SA . Therefore we will know the performance of the devices in addressing the APT. The devices are some analytic security devices that is Trend Micro Deep Discovery Inspector DDI and the Blue Coat Security Analytic SA . The parameters used for experiment scenarios are some types of malware which is distributed using free file sharing in the form of a URL link. The URL link will be downloaded by the target. Each security analytics tools are expected to recognize the threat and to obtain the detection rate of the security performance analytic tools. The larger the value, the better the performance of these devices. Each security analytics tools will identified the characteristic of the attack and were able to recognize the level of impact of the attack. The result shows that the performance of SA BlueCoat is better than TM DDI in term of detection rate for recognizing potensial malware in the first place. TM DDI is better than SA BlueCoat to recognize the characteristic of each malware.