Analisis Metode Keamanan Analitik Berbasis Security Information Event Management (SIEM) pada Teknologi Komputasi Cloud terhadap Serangan Advanced Persistent Threat (APT) = Analysis of Analytical Security Methods Based on Security Information Event Management System (SIEM) on Cloud Computing Technology Against Advanced Persistent Threat (APT)

Fatur Rahman Stoffel, author

Abstrak

Teknologi komputasi cloud merupakan sebuah pool besar yang terdiri dari sumber daya komputasi yang di virtualisasikan, sehingga pengguna dapat mengakses dan menggunakannya. Cloud telah diadaptasi oleh banyak perusahaan besar di bidang IT, seperti Google, IBM, Amazon dan masih banyak lagi. Oleh karena itu, keamanan pada teknologi cloud menjadi prioritas utama, sehingga bisa terhindar dari serangan cyber. Advanced Persistent Threat (APT) merupakan sebuah serangan cyber yang bertujuan untuk mendapatkan akses terhadap sistem atau jaringan, sehingga bisa melakukan pencurian data. Berbeda dengan teknik pencurian data biasa yang bersifat "smash and grab", APT akan tetap berada pada sistem target dalam periode waktu tertentu, sehingga penyerang bisa mengakses dan mengambil data target secara terus menerus, tanpa bisa terdeteksi. Hal ini membuat APT menjadi salah satu ancaman cyber yang sulit untuk dicegah, khususnya pada cloud environment. Metode keamanan analitik menjadi salah satu solusi yang bisa digunakan untuk bisa mengatasi serangan APT pada cloud environment, hal ini dikarenakan data yang dihasilkan semakin banyak, dan infrastruktur dari cloud juga mempunyai kapasitas yang besar untuk bisa menangani banyak nya data yang dihasilkan, sehingga metode keamanan lama yang sering diterapkan menjadi tidak lagi efisien. Salah satu metode keamanan analitik yang dapat diterapkan pada teknologi cloud adalah dengan menggunakan Security Information Event Management (SIEM) yang disediakan oleh banyak vendor seperti IBM dengan IBM QRadar. Hasilnya didapatkan bahwa kinerja tingkat deteksi SIEM dengan IBM Qradar terhadap ancaman serangan APT tidak optimal dengan pendeteksian hanya sebesar 57,1% dan yang terdeteksi sebagai kategori penyerangan sebesar 42,9% dari total 4 serangan yang dilancarkan. Hal ini dikarenakan IBM Qradar memerlukan beberapa ekstensi tambahan, sehingga membutuhkan resource komputasi yang lebih besar agar bisa meningkatkan kemampuan deteksi terhadap serangan APT.
.....Cloud computing technology is a large pool of virtualized computing resources, so that users can access and use them. Cloud has been adapted by many large companies in the IT field, such as Google, IBM, Amazon and many more. Therefore, security in cloud technology is a top priority, so that it can avoid cyber attacks. Advanced Persistent Threat (APT) is a cyber attack that aims to gain access to a system or network, so that it can carry out data theft. Unlike the usual "smash and grab" data theft technique, the APT will remain on the target system for a certain period of time, so that attackers can access and retrieve target data continuously, without being detected. This makes APT one of the most difficult cyber threats to prevent, especially in cloud environments. Analytical security methods are one of the solutions that can be used to overcome APT attacks in the cloud environment, this is because more and more data is generated, and the infrastructure of the cloud also has a large capacity to be able to handle a lot of data generated, so the old security method which are often applied become inefficient. One of the analytical security methods that can

be applied to cloud technology is to use Security Information Event Management (SIEM) that have been provided by many vendors such as IBM with IBM Qradar. The result shows that the performance of SIEM detection rate with IBM Qradar against APT attack is not optimal with only 57.1% detection rate and 42.9% detected as an attack category out of a total of 4 attacks launched. This is because IBM Qradar needs some additional extension, thus requiring more additional computing resources in order to increase the detection rate ability against APT attack.