Identifikasi tahapan serangan berdasarkan model Cyber Kill Chain menggunakan elastic stack: studi kasus Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah = Identifiying attack phase based on Cyber Kill Chain Model using Elastic Stack: case study of Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

Nana Mulyana, author

Abstrak

Sejalan dengan perkembangan teknologi, serangan terhadap dunia siber juga telah meningkat. Karenanya dibutuhkan sebuah kerangka atau model untuk memfasilitasi proses identifikasi serangan-serangan yang terjadi. Salah satu model yang dapat memfasilitasi proses identifikasi tahapan-tahapan serangan adalah Cyber Kill Chain (CKC). Cyber Kill Chain adalah sebuah model yang menggambarkan serangkaian tahapan sebuah serangan yang dilakukan terhadap sistem. Selain kerangka atau model, dibutuhkan pula sebuah alat bantu yang dapat digunakan untuk mempermudah proses identifikasi tersebut. Dalam tesis ini akan membahas proses identifikasi berdasarkan Cyber Kill Chain dengan menggunakan alat bantu berbasis platform open source yaitu Elastic Stack sebagai Security Information and Event Management (SIEM). Pemilihan penggunaan Elastic stack berdasarkan performa yang lebih baik dibandingkan dengan teknologi lainnya seperti Splunk, dimana penelitian yang dilakukan oleh peneliti lain mendapatkan hasil bahwa Elastic stack membutuhkan waktu sekitar 1 menit 14 detik, sedangkan Splunk membutuhkan waktu sekitar 1 menit 22 detik untuk 1 Milyar berkas log. Bentuk metode penelitian ini adalah penelitian kualitatif dengan metode studi kasus dengan melakukan simulasi untuk melakukan identifikasi tahapan-tahapan serangan. Dari simulasi ini, kita dapat menyimpulkan bahwa menggunakan Elastic Stack dapat membantu dalam proses mengidentifikasi tahapan serangan yang terjadi pada sistem dan infrastruktur sehingga dapat membantu dalam proses penanganan yang harus dilakukan untuk mengurangi risiko yang dapat diterima oleh pemilik sistem dan infrastruktur. Penelitian ini merekomendasikan kepada Lembaga Kebijakan Pengadaan barang/jasa Pemerintah Direktorat Pengembangan Sistem Pengadaan Secara Elektronik selaku pengelola sistem informasi untuk proses pengadaan, untuk melakukan implementasi Security Information and Event Management (SIEM) menggunakan Elastic

.....In line with technological developments, attacks on the cyber world have also increased. Therefore we need a framework or model to facilitate the process of identifying the attacks that occur. One model that can facilitate the process of identifying stages of attack is the Cyber Kill Chain (CKC). Cyber Kill Chain is a model that describes a series of stages of an attack carried out on a system. In addition to the framework or model, it also needed a tool that can be used to facilitate the identification process. This thesis will discuss the identification process based on the Cyber Kill Chain using open-source platform based tools, namely Elastic Stack as Security Information and Event Management (SIEM). The selection of using the Elastic stack is based on better performance compared to other technologies such as Splunk, where research conducted by other researchers found that the Elastic stack takes about 1 minute 14 seconds, while Splunk takes about 1 minute 22 seconds for 1 billion log files. . While this research is a qualitative research with a case study method by conducting simulations to identify stages of attack. From this simulation, we can conclude that using Elastic Stack can help in the process of identifying stages of attacks that occur on

systems and infrastructure so that it can assist in the process of handling that must be carried out to reduce the risks that can be accepted by the system and infrastructure owner. This study gives a recomendation to Directorate Pengembangan Sistem Pengadaan Secara Elektronik of Lembaga Kebijakan Pengadaan barang/jasa Pemerintah as the management of the information system for the procurement process, to implement Security Information and Event Management (SIEM) using Elastic Stack.