Abstract

The cybercrime is hard to be investigated and performed, which encouraged the cyber attackers. The actors from the cyber attacks evolved from small individuals passionate about IT and Governments willing to control the cyber space to offenders who found a new space to explore. The attacks became more and more sophisticated and organized, and the government decided to invest in methodologies and instruments to prevent and control such attacks. The chances for defence were always smaller than the chances for attack. The nowadays instruments used for detecting the breaches from a system used various technologies for the detection and removal of the unsecured code and with malicious purpose before reaching the infrastructure of the organization. Those instruments, in exchange, offered the attackers the chance to build attack instruments against the defence measures. The methods of traditional approach in the cyber security were efficient in the past, being given the fact that those were based on the defence of the perimeter with detection instruments based on signature. Nowadays, these instruments cannot face these new types of attack. Even though these vulnerabilities are discovered and reported, usually, it takes a long period of time until a patch is delivered by the providers and installed by the organizations. The instruments as the management of the information and events security (SIEM) allow the organizations to consolidate the data from more security devices in one system. But, SIEM is efficient only in the environments with enough personnel and power to process close to the support of investigation and analysis. Moreover, such systems do not function correctly due to the large quantity of data and the extremely reduced analysis. Many times, the majority of data is simply archived. The instruments of analysis on large quantities of data and the low calculation power opened up new opportunities in the cyber space. While the attackers can change the instruments and the approaches, their operation methods remain mainly the same. This behavioral constant allows the analysis technologies detect the malicious attacks in a shorter time. These systems take into consideration the users profile, the business behavior and norms to set out the thresholds in which the events can be considered abnormalities. The traditional security instruments function using predefined patterns and scenarios modelled depending on the attacks from the past to detect and block the suspicious behaviors. The data analytics can report to how a normal daily behavior is and can indicate abnormalities as a calculator which suddenly downloads very large files. The statistic correlations based on events do not depend of the already existing knowledges of a problematic activity, but it is based on the recognition of what a normal activity represents. Using advanced mathematical models, a normal environment is modelled such that the activities which deviate from the normal path are between a well-established statistic range and the defense mechanisms are set off automatically. What is considered normal can be abstracted up to the users profile level. Based on the mathematical models, the users are grouped depending on many features and have a basic limit which is established for that group of users. The network behavior which deviates from the group features suggests irregularities and future information. Despite the challenges concerning the normalization of a large quantity of information from dynamic and different sources, big data will always play an important role in security. By its incorporation in the security programs, the organizations create a richer context for the minimization of risks and learn what is normal in the activity of a certain type of user, group or process. The cyber security is a constant process of reaction to possible threatens while adapting to the new requirements and needs of an organization. Cybersecurity analytics can improve the prevention and can reduce the time between the incident and detection. The key components of such a system are: data sources, data storage medium, interface with data, analysis engine and presentation.