Chapter 5
A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools

Manjunath Kotari
Alva's Institute of Engineering and Technology, Moodbidri, India

Niranjan N. Chiplunkar
NMAM Institute of Technology, Nitte, India

ABSTRACT

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

1. INTRODUCTION

Cyber security threats are major hurdle for the development activities of the Information Technology (IT) industry. The IT industry is facing severe crisis of cyber-crime activities in their business. A large set of data and assets of organizations are placed in cloud-based platform. The virtual cloud computing is facing various threats which include, Intrusions, Malwares, and Mining of Crypto currency. The

DOI: 10.4018/978-1-7998-2242-4.ch005

Virtual Machines faces intrusions and impersonations in the cloud environments. The bitcoin attracts more severe cyber crimes. This can be illustrated in cloud computing by layer wise cyber attacks. Cyber Security (Gupta, Agrawal, & Wang, 2019) is becoming a very important concern for the functioning of web applications. The rising cost of cyber security damages reflects a failure of the security field to offer a solution that is both simple enough to warrant adoption by industry and government and secure enough to protect our valuable assets and data. Most of the organizations are facing shortage of cyber security professionals to monitor the user activities in day to day life. However, IT organizations may use various tools and technologies to maintain privacy of user data. Most of the corporate information security (Quhtani, 2017) is analyzed by data mining applications. In the corporate world, marketing campaign surveys are analyzed according to data mining applications. The objective of this chapter is to provide the comprehensive survey on detection and analysis of various cyber security threats exists in the web applications and network. The chapter also reviews the various open source security monitoring tools with classifications. The challenges faced by cyber-security tools have been included for the purpose of providing future solutions. The architecture of cyber-security threat detection and monitoring system to analyze the working of cyber-security tools has been proposed in this chapter.

1.1 Cyber Security Monitoring

Security monitoring is the collection of data from a range of security systems and the correlation and analysis of this information with threat intelligence to identify signs of compromise. Cyber-Security monitoring is an essential part of cyber risk management systems, which enables the company networks to detect cyber hackers in their early life, and quickly shoot up threats for healing before they cause harm and interference. Baselining is the process of establishing an agreed level of typical network performance. It plays an important role in cyber security monitoring. Any network behavior that falls outside what is considered regular behavior should be analyzed to identify whether or not it could be malicious.

1.2 How Does Cyber Security Monitoring Work?

Cyber security analysts will utilise a range of technologies to achieve visibility of threats. There are two types of monitoring, viz., network security monitoring and endpoint security monitoring. Network security monitoring tools comprise Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS). SIEM systems collect, manage and correlate log information from a range of sources to provide a holistic view of security posture, and generate alerts for investigation by cyber security analysts. IDS combines network (NIDS) and host (HIDS) based methods to analyse network traffic and identify anomalous behaviour. Endpoint security monitoring technologies provide visibility of activity such as file read, write, executions and registry changes across desktops, laptops, and servers.

1.3 Challenges of In-House Security Monitoring

Basically all the security monitoring tools generates enormous number of alert messages. Filtering of alert messages to identify true threats from false positives is hassle task. In that case, essential alerts may be ignored during the monitoring process. Hence, setting up of new Cyber Security Operations Centre (CSOC) is essential. However, CSOC is more expensive. Instead of recruiting, training and managing