Advanced hunting and content development

Technology, Information Technology

Advanced Hunting and Content Development Synopsis of the Advanced Hunting and Content Development Evidently, in an era characterized by big data and hacking, companies require the best tools, people, organizational focus, and people to benefit from the right capacities for data mining and acquisition of insights relevant facilitating better decisions and value creation (Talabis, McPherson and Martin 3). For effective advanced hunting, companies are expected to use different tools or mechanisms to identify any malicious activity against their big data, and establish an automated tool for use in content development.

However, most skilled antagonists manage to access defenders' tools and resources or to some extent evade such tools causing anomalies in big data or engaging in fraud. Attack or evading defenders' tools involve using counter infrastructure and tools that compromise data. Defenders must then have indicators of compromise (IOC) such that their content identifies methods or numerous pieces of evidence (Orlando 23). This introduces the need to distinguish between analytic and hunting where analytics include the means of obtaining attractive objects, patterns, and events, and this is supported by hunting together with monitoring. However, monitoring is not analytics, but ensuring that the system is free from evident or hidden compromise by offenders. In their attack, offenders use different platforms and phishing techniques while defenders are forced to use such as exploit kit servers such as RSA Security Analytics to monitor phishing and other attacks.

RSA security analytics work toward protecting phishing, and suspicious objects, patterns or events using notifications such as warnings, provision of

information, and curbing suspicions. In all cases, RSA security analytics uses an event reconstruction to identify suspicions, warnings, or compromise, and communicates to the present security tools including intrusion prevention systems, and firewalls. The security tools are also informed of things that present threat to the system (Musthaler n. p).

Security Analytic Tools

The two identified are Zenoss Core, Network Miner, and angry IP Scanner. The Zenoss Core platform combines system management and integrated network analysis of performance, events, availability, and configuration. The platform uses simple protocols for streaming data through SSH, JMX, and Syslong for flexible foundation to manage events and monitor logs. In addition, the tool offers features that are particularly geared towards virtual and cloud infrastructure.

Network minor tool offers a great way of scrutinizing files, chat history, searching files, and identifying odd cookies and agents (Netresec n. p). The implication is that Networkminer is not about network traffic monitoring, but analysing network forensic for windows, while collecting data regarding the host network unlike its traffic. The technique used involves sniffing for packets to ascertain that users are assisted in detecting OS, open ports, and host names within the network.

The Angry IP Scanner relies on a scanning technique that uses multi-threaded scanning methods, thus offering speedy scans (Angry IP Scanner n. p). The results can be saved in the form of. txt, . csv, . xml, and list files for IP ports. Since the tool utilizes flexible java-based framework, it is easily extensible using plug-ins that gather additional information regarding

scanned IPs.

Works Cited

Analytics and Content Development. Dir. Mark Orlando. 2013.

Angry IP Scanner. What is it? 28 May 2015. .

Musthaler, Linda. " Security analytics will be the next big thing in IT security." Network World 31 May 2013: xx.

Netresec. Netresec Network Security Blog. 20 October 2014. .

Talabis, Mark, Robert McPherson and Miyamoto Martin. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. London: Elsevier Science & Technology Books, 2014.