Cyber Threat Intelligence and its Role in Proactive Incident Response

Husam Hassan Ambusaidi[a] and Prakash Kumar[a],

Every day organizations are targeted by different and sophisticated cyber attacks. Most of these organizations are unaware that they are targeted and their networks are compromised. To detect the compromised networks the organizations need a reliable source of cyber threats information. Many cyber security service vendors provide threat intelligence information to allow early detection of the cyber threats. This research will explore different type of cyber threat intelligence and its role in proactive incident response. The research study the threat intelligence features and how the threat feeds collected and then distributed. The research studies the role of cyber threat intelligence in early detection of the threats.

Keywords: Cyber Attacks; Intelligence; Proactive;Incident Response; Malware; Viruses; worms;

Introduction

Nowadays information technology involved in every aspects of our life. The critical information is flowing all around and the protection of this information became a big challenge for cyber security experts. The critical information that requires protection distributed in different IT systems such as internet of things systems, health sector systems, airports systems, Finance sector, etc. As the number of systems, increase the threats to these systems increasing. To allow better and prompt actions against these threats, the cyber security service providers have introduced the Cyber Threat Intelligence. The cyber Security Threat Intelligence is "is the knowledge of threat's motives, resources, capabilities, and goals" [1]. The cyber threat intelligence becomes one of the most important factors in every cyber security incident response strategy. The Cyber security service provider Symantec has published report shows that in 2016 approximately 229,000 is the average number of web cyber-attacks detected daily by the organizations around the world [2]. By providing reliable threat intelligence information high majority of cyber-attacks can be detected proactively.

Threat Intelligence Platform

Due to the high sophisticated cyber threats, cyber threat intelligence plays an important role to defend against these threats. Information Technology companies such as cisco with its TALOS organization, Symantec's DeepSight Security Intelligence Solutions, and FIREEYE's ISIGHT threat intelligence are examples of the cyber threat platforms that are available in the market. The threat intelligence platforms use different methods to collect, analyze, and distribute cyber threats information.

Cisco's TALOS

TALOS is an organization established by Cisco for the purpose of cyber threat intelligence. TALOS working in five major areas threat intelligence, detection research, vulnerability research and outreach, engine development, and development. TALOS analyze the cyber threats across web, networks, cloud environments, emails, and end points. After analyzing these threats TALOS share a complete understanding of cyber threats, scopes of outbreaks, and their root causes with its customers. TALOS is continuously detecting and searching for new cyber threats. When new threats are discovered, TALOS releases advisories and rules to protect against these threats. By providing such information, the possibility to response to such threats proactively is increased [3].

Symantec's DeepSight

Symantec's DeepSight is a cyber threat Intelligence solution grant customers with relevant, timely, reliable intelligence information regarding emerging threats, threat sources and vulnerabilities to enable incident response teams to keep up-to-date with the changing threat. DeepSight collects information from more than 240,000 sensor monitoring different networks in more than 200 countries around the world, more than 133,000,000 Symantec technology products and services, visibility into all internet ports/protocols for threat collection and analysis, over 8 billion emails tested per day, and over 1 billion web requests daily [4]. By having large number of sensors and information gathering agents, DeepSight allow better and broad threat intelligence from different sources. DeepSight give Symantec's customers the advantage of timely and reliable threats information with suitable countermeasures.

FireEye iSIGHT

iSIGHT is a wide, broad threat intelligence across all classifications of threats such as (critical infrastructure , cyber espionage, cyber crime, hacktivism, and much more). iSIGHT brings visibility over an extended cyber attacks life cycle based on an unmatched view across attackers, victims, and networks around the world [5]. FireEye has established the iSIGHT solution to be dynamic, which allow integration with different levels of threat intelligence.

The Role of Threat Intelligence in Poractive Incident Response

a. Department of Electronics and communication Engineering, Middle East college, Muscat
Correspondence: prakash@mec.edu.om

To respond to any cyber incident, incident responders must follow several procedures to manage the incident. Incident management phases are Prevention, Detection, Response, and Reporting.

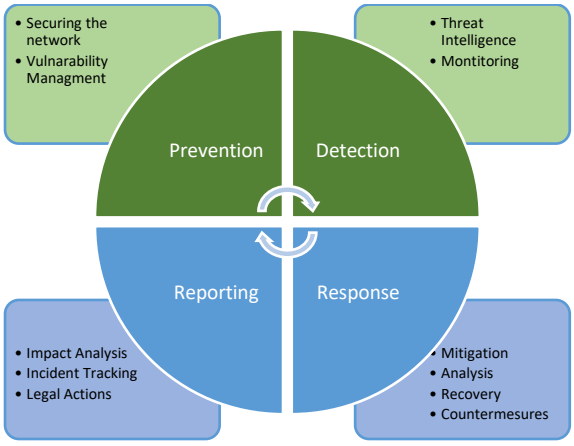

Figure. 1. Incident Response Management life Cycle

Incident response is a critical task to recover from cyber incidents and react to threats. In prevention and detection phases of incident response procedures incident response teams needs sufficient information about cyber threats that they face. Cyber threat intelligence allows incident responders to prevent form threats and react to incidents in many ways:

Vulnerability intelligence

Threat intelligence platforms offer timely and different vulnerability information from different vendors. Using such information allow prompt vulnerability patching and bug fixes. This mechanism prevent attackers from exploiting the vulnerabilities that are exist in the systems as it allows fast patching and fixes[9].

Malware codes/signatures Intelligence

Using the sensors that deployed around the world networks, threat intelligence providers collect information about new malwares, viruses, Trojans, and worms. After collecting the information, the analysis of these malwares will take place. Then signatures and codes of these malwares will be shared among customers to allow better prevention against these malwares [6].

Black listed IPs/domains and URLs intelligence

This type of threat intelligence monitor the Internet Addresses (IPs), domains, and URLs that are malicious or used to conduct malicious activities [8]. After collecting information about this IPs and domains, the intelligence information will be forwarded to the customers to enable them to do better prevention.

By providing such information, the incident response will be more effective due to different factors such as timing, accuracy, and relevance. The threat intelligence platforms share feeds about emerging threats with consideration to the timing to allow prior prevention and countermeasures. The accuracy factor will allow incident responders to know the exact threat and its characteristics and behavior. The relevance factor allows the incident responders to know the effect of these threats and what the suitable countermeasures [7].

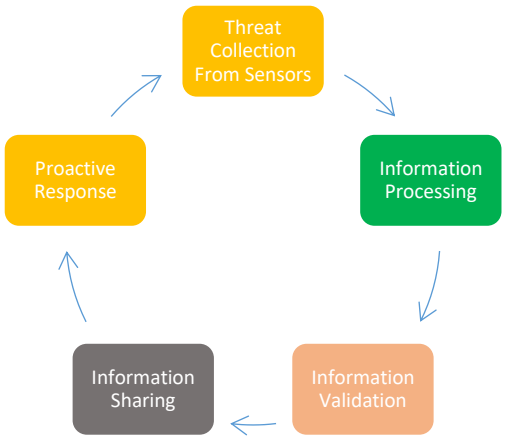

Fig. 2. Threat Intelligence Life Cycle

Importance of Threat Intelligence Platforms

The cyber space is full of threats that may well affect any organization at any time. Cyber threat intelligence should be an important part in every organization incident response plan and overall information technology security strategy. The role of cyber threats intelligence can be summarized in the below points:

- It allow faster protection against emerging threats in the cyber space
- The detection of undiscovered security breaches and malware infections will be easier.
- Allow the automation of incident response using smart response.
- Give the organization better monitoring view to their networks.

Conclusion

This paper has explored the different types of cyber threat intelligence platforms available in the market. The paper also addressed the role of threat intelligence in proactive incident response. The outcome of this paper is identifying the advantages of using cyber threat intelligence. In conclusion, cyber security is rapid changing field were the experts, professionals, and IT security service providers need to be invocative and up to date to be aligned with emerging threats.

Acknowledgment

I am very much thankful to Middle East College, Muscat for providing me lab facilities and also creating an environment of renowned professors who helped me at every step during contribution to my work and defining me new research findings related to the work proposed

References

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113–125;

AMIN,R.M.,RYAN,J.,H,J.C.,AND VAN DORP,J.R. Detecting Targeted Malicious Email. IEEE Security & Privacy 10,3(2012),64–71.

J. Jose, J. Jose, F. Jose, "A survey on secure data aggregation protocols in wireless sensor networks", International Journal of Computer Applications, vol. 55, pp. 17-21, October 2012.

B. Koldehofe, F. Dürr, M. A. Tariq, K. Rothermel, "The power of software-defined networking: Line-rate content-based routing using openflow", Proceedings of the 7th Workshop on Middleware for Next Generation Internet Computing, ACM, pp. 3:1-3:6, 2012.

Threat Connect, "THREAT INTELLIGENCE PLATFORMS Everything You've Ever Wanted to Know But Didn't Know to Ask", Threat Connect, Arlington, 2015.

FIREEYE ISIGHT THREAT INTELLIGENCE SCALABLE THREAT INTELLIGENCE FOR ADDED CONTEXT ACROSS THE ORGANIZATION, 1st ed. FIREEYE, 2016, pp. 1-3.

Symantec DeepSight Security Intelligence Solutions, 1st ed. Symantec, 2012, p. 1.

Symantec, "Internet Security Threat Report", 2017.

TALOS Group, 1st ed. TALOS Intelligence, 2016, pp. 2-4.