Chapter 5
How Cyber Threat Intelligence (CTI) Ensures Cyber Resilience Using Artificial Intelligence and Machine Learning

Neelima Kant
Sharda University, India

Amrita
Sharda University, India

ABSTRACT

Cyber threat intelligence (CTI) has emerged as a critical pillar in a well-developed cyber security strategy. When used correctly, threat information may assist security teams in defending against an ever-more sophisticated threat landscape before, during, and after an attack. Groups can design more effective, more delicate, and durable cyber defenses by evaluating attackers and understanding their methods and aims. As a result, the purpose of this chapter is to give an overview of how CTI promotes cyber resilience by utilizing intelligent technologies such as artificial intelligence (AI) and machine learning (ML).

INTRODUCTION

Cyber Threat Intelligence is data that helps a company better understand the risks that have been, will be, or are currently being directed at it. This information is used to anticipate, prevent, and identify cyber-threats attempting to exploit valuable resources. Six reasons why CTI is so important:

- Lowering Costs - Because enhanced defenses help to limit an enterprise's risk, CTI can lower overall costs and save commercial firm funds.

DOI: 10.4018/978-1-6684-3991-3.ch005

- Lowering Risks - CTI gives the correct visibility into emerging security threats, reducing the risk of data loss, minimizing or preventing disruption in company operations, and ensuring regulatory compliance.
- Prevent data loss - CTI works as a watchdog when questionable IP addresses or domains seek to communicate with the community in order to capture vital information.
- Maximizing staffing - CTI increases an employer's safety crew's productivity by connecting threat intelligence with anomalies identified by network technologies.
- In-depth Threat Analysis – CTI allows a business to study a cybercriminal's various approaches. The employer can determine whether the safety protection systems can block such attacks by examining such cyber risks.
- Threat Intelligence Sharing - Sharing critical cyber security information, such as how hackers plot a security breach, could help others avoid a similar attack. The more the company is able to thwart these attempts, the less likely the hackers are to carry out such heinous attacks.

BACKGROUND

Researchers have been using various artificial intelligence (AI) and machine learning (ML) techniques to find cyber-attack indicators, malware evaluation, and anomaly detection techniques in recent years. With the advancement of IoT technology, the number of IoT devices/sensors has significantly expanded. Large-scale sensor-based structures are expected to become more prevalent in our societies, necessitating the development of creative approaches for designing and operating these new structures. The Cloud is migrating to the edge of the network, where resources such as routers, switches, and gateways are being virtualized, to help with the computational call of real-time delay-sensitive packages in large part dispersed IoT devices/sensors.

There are 6 major databases (Google scholar, IEEE Explore, ACM Digital Library, Science Direct, Web of Science, Scopus) used in (Xiong & Lagerstrom, 2019; Mckinnel et al., 2019) for providing the systematic literature review on Threat Modelling and AI in Vulnerability analysis and Penetration Testing. The study provides a lot of scope and challenges in cyber security using AI and ML techniques. Viz.

- Direct applications of vulnerability analysis and penetration testing using AI and ML
- Used real data for analysis of false positive rates using different approach and techniques in different research papers.
- It also covers partial applications of AI and ML, used by different researchers.
- Used peered review conferences and journal papers for meta-analysis and literature survey.

Author states that the most of threat modelling work has been done manually, so assuring on validation of results is quite a difficult job. For this literature survey, almost 176 articles published between 2004 to 2021 have been covered, out of which 54 are identified for future prospects for research.

On time recovery, it is mandatory to gather the real time cyber data to block the attacks. For most of the organizations, the technicality behind the Threat Intelligence is actually required. As per (Tounsi & Rais, 2018), the new generation attacks are more complex to handle than earlier attacks. It is necessary to create a boundary for cyber defense for new threats.