Chapter 2
Improving Cyber Threat Intelligence Through Generative AI From Data to Actionable Intelligence

Vijay Singh Rana
http://orcid.org/0009-0006-0234-2225
J.V. Jain College, Saharanpur, India

Tarun Kumar Vashishth
http://orcid.org/0000-0001-9916-9575
Department of Computer Applications, Vidya University, Meerut, India

Puneet Chauhan
http://orcid.org/0009-0000-1652-8764
School of Computer Application, Swami Vivekanand Subharti University, Meerut, India

Vikas Sharma
http://orcid.org/0000-0001-8173-4548
Department of Computer Applications, SRM Institute of Science and Technology, Delhi NCR Campus, Ghaziabad, India

Sachin Tomar
Department of Computer Applications, SRM Institute of Science and Technology, Delhi NCR, India

Shahanawaj Ahamad
College of Computer Science and Engineering, University of Hail, Saudi Arabia

Aditi Chauhan
School of Humanities and Mass Communication, IIMT University, Meerut, India

ABSTRACT

Cyber threat intelligence (CTI) is of great importance in the proactive nature of the cyber defense process, allowing organizations to make actionable plans for evolving

DOI: 10.4018/979-8-3693-8397-1.ch002

threats. Historically, acquiring cyber threat intelligence has been beset by the lack of comprehensiveness, immediacy, and the ability to synthesize disparate data from undefined sources of threat intelligence. Generative AI affords an opportunity to rise above these deficiencies from the perspective of the depth, speed, and readability of threat intelligence. This chapter assesses how generative AI may be of assistance in driving forward the study of cyber threat intelligence from the millennial perspective, but from an initial perspective – how generative models do indeed have the capability of producing threat hints and warnings, modelling essential threat/attack scenarios and augmenting sources of data for training detection systems.

1. INTRODUCTION

The current complexity and range of modern cyber threats have proliferated into unimaginable proportions. The organisations in today's environment are faced with a volatile environment of advanced persistent threats (APTs), ransom ware activities, phishing attacks and other sponsored cyber-attacks. It is evident that the traditional measures have an estimable role, failing typically against the difficult and complex nature of these attacks. Most organisations are looking to Cyber Threat Intelligence (CTI), that is the structured collection, evaluation and analysis of information related to threats, with a view to assisting in informed decisions and act proactively in the fight against these threats. (Vemuri et al., 2024).

1.1 Background on Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) essentially involves the structured collection, processing and analysis of information pertaining to the salient threats to the digital environment of the enterprise at hand, either real, or to be. Converting disparate and uncollected security information into useful information for the purpose of assisting in better decision making of intelligence outcome, and to optimise the cybersecurity activities of the enterprise, is the main purpose of CTI (Saurabh et al., 2024). The better able an enterprise is to know the tactics, techniques, and procedures of its adversaries, the better able it is to foretell attacks on them, enhance their defensive levels and maintain exposure to the risk. The growing importance of CTI is closely related to the growing and sophisticated cyberattack landscape that is based on polymorphic malware, supply chain exploitation and zero-day exploits that evade most of the classical means of defence used. CTI is a proactive means to secure one's organization as it changes the focus from a purely reactive incident response model to a preventive means of reducing the risk of security threats before those threats pose larger problems. That is usually divided by a three tier means to provide