

Cyber Threat Intelligence: A Comprehensive Overview and Practical Implementation

Sushama Pawar¹, Yogita Khandagale², Archana Gopnarayan³, Manisha Pokharkar⁴

Lecturer, Information Technology^{1,2,3}

Lecturer, Computer Engineering⁴

Vidyalankar Polytechnic, Mumbai, India

sushma.pawar@vpt.edu.in

Abstract: *Cyber Threat Intelligence (CTI) has emerged as a critical component in modern cybersecurity strategies. CTI encompasses the proactive gathering, analysis, and dissemination of information about potential cyber threats, including threat actors, tactics, techniques, and procedures (TTPs), vulnerabilities, and indicators of compromise (IOCs). By harnessing a combination of technology, human expertise, and collaborative partnerships, CTI enables organizations to enhance their ability to detect, prevent, and respond to cyber attacks effectively. This paper provides a comprehensive examination of CTI, including its definition, importance, lifecycle, sources, and practical implementation strategies. By exploring various CTI frameworks, methodologies, and tools, organizations can effectively leverage threat intelligence to enhance their security posture and proactively defend against cyber threats.*

Keywords: Cyber Threat Intelligence, CTI, Threat Intelligence, Cybersecurity, Intelligence Lifecycle, Threat Detection