IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, December 2025
Impact Factor: 7.67

Optimizing Threat Intelligence Analysis

Prof. Rahul Raut[1], Mansi Mahamuni[2], Snehal Jadhav[3], Arya Nandgude[4]
Professor, School of CSIT (Cybersecurity)[1]
Student, School of CSIT (Cybersecurity)[2,3,4]
Symbiosis Skills and Professional University, Kiwale, Pune

Abstract: *The fast increase in the amount of Cyber Threat Intelligence (CTI) means there's a need for a well-organized, scalable solution that helps organizations analyze this information effectively. Current methods often depend on manual and separate processes for collecting data, which leads to slow responses and problems in connecting different threat details. The main aim of this project was to successfully set up the Optimizing Threat Intelligence Analysis Platform, an open-source system, making it the main central place for organizing, connecting, and showing different types of CTI data. The process involved using Docker Compose to deploy the Optimizing Threat Intelligence Analysis application stack, and integrating key services like the main platform, Elasticsearch for quick data indexing, and RabbitMQ for dependable message handling. The main framework used the STIX 2.1 standard for sharing information and the MITRE ATT&CK framework for categorizing how attackers operate. Data was tested and confirmed through different ways, including uploading pre-made STIX 2.1 JSON files for detailed threat networks and making CSV Mappers to automate the input of simple Indicator of Compromise (IOC) lists. By carefully setting up the system, the built-in dashboard was adjusted to use the platform's graph database features, allowing for clear visualization of connections between Threat Actors, Campaigns, and Indicators. The final system creates a unified knowledge graph that greatly improves how quickly and accurately threats can be investigated and monitored. The project's outcome shows that Optimizing Threat Intelligence Analysis is a strong tool for organizations looking to improve their intelligence-based defense approaches*

Keywords: Cyber Threat Intelligence (CTI), CTI Optimization, STIX 2.1, Knowledge Graph, Automation, Threat Intelligence Platform (TIP), Optimizing Threat Intelligence Analysis , TTPs (Tactics, Techniques, and Procedures)

DOI: 10.48175/IJARSCT-30379