DYNAMO

Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors

Follow DYNAMO on:

@DYNAMO_HEU

dynamo_horizon

Factsheet 2: Cyber Threat Intelligence

The development of the DYNAMO platform enables the resilience assessment of the critical sector by combining the disciplines of Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI). The combination of CTI processing with the BCM approaches will further enhance situational awareness and recovery planning capabilities of Businesses/Critical Infrastructures. What exactly is meant by Cyber Threat Intelligence and how this discipline is built into DYNAMO is explained in more detail in this edition of the DYNAMO factsheets.

Cyber Threat Intelligence in a Nutshell

Cyber Threat Intelligence (CTI) is information based on knowledge, skills and experience to help mitigate potential attacks and harmful events in cyberspace. The discipline aims to identify cyber-attacks affecting physical or cyber-physical elements and threat actors and understand their motives, objectives and approaches. The results and findings are processed to evaluate also on the basis of new information and feedback from users. In any case, in recent years, Cyber Threat Intelligence has become an important part of corporate and public sector cyber security operations, as it enables them to be more proactive at the tactical, operational and strategic levels and to identify which threats represent the greatest risks to them. CTI also helps to share trusted information about various threats with the right parties in a timely manner to support the search for strategies. Proper application of cyber threat intelligence can provide better insight into cyber threats and enable faster and more targeted response, development and allocation of resources.

The DYNAMO CTI approach

DYNAMO aims to identify threats for the three use cases in the health sector, energy supply and the maritime with the help of CTI through the developed platform. The goal is to develop timely, relevant and actionable information on new and emerging threats, combined with the BCM approach, so that sectors can improve cyber security posture by updating their security measures and train their personnel against current and emerging threats. The DYNAMO platform will collect, extract, analyse and share actionable CTI from both internal and external sources. Internal sources that will be used are logs from various security tools available to the organisation. External online sources include feeds from intelligence sharing communities, as well as semi-structured and unstructured online sources. Data collected through the Threat Intelligence Sharing Platforms (TISPs) and other sources will be correlated and analysed in order to improve the situational awareness and allow faster prevention, response and identification of the mitigation techniques. The solutions will be integrated into the Cyber Knowledge Graph to enable graphical representation and interactive analysis of threat data, past and likely future impact on the organisation and improve its situational awareness. But more on the situational awareness can be found in the next Factsheet issue.

DYNAMO Platform is equipped with a variety of tools that contribute to the design of a robust and finely organized CTI solution. The DYNAMO CTI suite comprises of a range of tools with diverse functionalities, aimed at establishing a seamless flow from incident detection to information gathering and appropriate response. The CTI solution cycle begins with incident detection. The DYNAMO suite includes two tools that contribute to that cause. Cyber-attack forecasting (CAF) tool provides predictive analytics based on ML and AI algorithms. CAF forecasts cyber-attacks activities within the next minute, making it a pro-active tool. Secure AI also enables the detection of cyber events, however its functionality is based on the analysis of collected data using state-of-the art ML algorithms to form a more detailed report on a possible incident. In order for that information to be completely explicable to the system administrators, SecureAI provides also some visualization modules. Besides that, there is also a dedicated tool for visualizations purposes, called ThreatLens, which provides users an interactive way to acquire insights about potential attacks, threats and vulnerabilities into their systems. It will be developed with a clear and robust approach to visualizing information using visual analytics and Natural Language Processing. A crucial part of the CTI solution circle is the information sharing. The CTI Extractor is responsible for the collection, extraction, analysis and correlation of CTI from both several external (i.e., online), as well as internal sources. Additionally, the Early Warning System (EWS) serves the purpose of sharing cyber-incident information in near real-time, providing a support tool for security operations that facilitates coordination among personnel. Operators will thus be able to assess impacts, identify and evaluate mitigation actions and prioritize response measures. DYNAMO's CTI suite also includes a cyber security intelligence management system, Cyber Knowledge Graph (CKG), which collects and correlates threat intelligence related information from various sources and maps it to the concepts of a cyber security ontology. Last but not least the suite includes a Data Anonymization tool consisting of a unified web interface and a simple, flexible and configurable anonymization engine, which will enable the secure handling of datasets inside the DYNAMO platform.

Fraunhofer EMI · TECHNIKON · Information Technologies Institute · factorSOCIAL · Laurea University of Applied Sciences · NAVAL GROUP · Gemelli · KEMEA · KPMG Future Analytics · VISIONSPACE · telelink Business Services · RHEA · UCC · CRBC · CUBS · SystemX · Laborelec

Consortium
15 Partners
10 Countries

Budget
€ 5 Million
100% EU-funded

Duration
36 Months
10/2022 - 09/2025

Funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.