Lehrstuhl für Wirtschaftsinformatik I
Informationssysteme
Prof. Dr. Günther Pernul

Contributions to Cyber Defence

Industrial research project funded (2019 - 2022)

Contributions to Cyber Defence is a research project aimed at the analysis and advancement of structured data formats in the context of Cyber Threat Intelligence (CTI). Due to the increase of sophisticated attacks on various IT systems there is an urgent need to structure, share and apply threat information for defensive measures. Incidents described in a structured data format can be shared more easily via dedicated sharing platforms and the subsequent application in different organizational settings can help to prevent the spreading of attacks. In addition, legal obligations mandate critical infrastructure operators and certain industry sectors to report incident information to governmental supervisory institutions.

Based on the aforementioned aspects the research approach covers:

1. A detailed analysis of requirements in the field of Cyber Threat Intelligence in conjunction with specific data formats.
2. The comparison of relevant data formats will build the basis for an in-depth evaluation of advantages and disadvantages of these data formats.
3. An integrative approach will address data format specifics and the advancement towards a unified standard. Contributions to Cyber Defence will also focus on linking elements to a procedural incident model.
4. The prototypical implementation will pursue technical aspects of the data format related findings. Additionally, there will be an evaluation with real-world datasets to show the feasibility of the proposed solution.
5. Legal aspects will be considered as they may hinder the application in real-world use cases.

The Contributions to Cyber Defence will result in a detailed analysis of structured data formats in Cyber Threat Intelligence and related aspects as well as a prototypical implementation. The outcome will ensure actionable CTI and the support of further use case scenarios.

The project started on April 1, 2019 and will run over a period of 3 years.