Unifying Cyber Threat Intelligence

The threat landscape and the associated number of IT security incidents are constantly increasing. In order to address this problem, a trend towards cooperative approaches and the exchange of information on security incidents has been developing over recent years. Today, several different data formats with varying properties are available that allow to structure and describe incidents as well as cyber threat intelligence (CTI) information. Observed differences in data formats implicate problems in regard to consistent understanding and compatibility. This ultimately builds a barrier for efficient information exchange. Moreover, a common definition for the components of CTI formats is missing. In order to improve this situation, this work presents an approach for the description and unification of these formats. Therefore, we propose a model that describes the elementary properties as well as a common notation for entities within CTI formats. In addition, we develop a unified model to show the results of our work, to improve the understanding of CTI data formats and to discuss possible future research directions.