INDICAETING

INtrusion DetectIon by Correlating Automatically Extracted Threat INtelliGence

Programm / Ausschreibung	FORPA, Forschungspartnerschaften NATS/Ö-Fonds, FORPA NFTE2018	**Status**	abgeschlossen
Projektstart	01.10.2018	**Projektende**	30.06.2022
Zeitraum	2018 - 2022	**Projektlaufzeit**	45 Monate
Keywords	cyber security, cyber threat intelligence, anomaly detection, log data analysis, information extraction		

Projektbeschreibung

Threat Intelligence consisting of Indicators of Compromise and Tactics, Techniques and Procedures is of uppermost importance for identifying cyber threats using signature-based detection techniques. However, large IT infrastructures are often insufficiently protected due to the fact that such approaches rely on predefined attack dictionaries that have to be maintained manually, which requires time- and resource-consuming activities as well as expert knowledge about the attack itself and the system at hand. For this reason, the main goal of this project is the definition of a methodology for an automatic or semi-automatic extraction of actionable Threat Intelligence from raw and unstructured log data allowing timely reaction to immanent threats. The proposed approach is thereby able to gather security-relevant information about previously unknown attacks using self-learning Anomaly Detection techniques that process log streams from arbitrary sources in real time. Correlating the identified anomalies across multiple layers and diverse systems reduces false alarms and enables that multi-stage intrusions comprising complex dynamic patterns are enriched with information about the context and the circumstances of attacks in order to provide comprehensive protection for all participants making use of the insights shared on public threat intelligence platforms.

Projektpartner

- AIT Austrian Institute of Technology GmbH