Automating Attack Data Labeling with Generated Rules and Anomaly Detection

Rémi Bouchayer*[1]

[1]Institut Polytechnique de Paris (IP Paris) – Institut Polytechnique de Paris, Télécom Sud Paris, 91000 Courcouronnes, ECE Paris – Route de Saclay, 91120 Palaiseau Cedex, France, France

Abstract

The development of artificial intelligence augmented detection systems is constrained by the availability of data.

In order to train and evaluate models, it is necessary to have a large number of representative but diverse examples.

Normal data can be generated from simulations of representative information technology infrastructure.

Threat emulation is a process that generates realistic attack data.

Various attack scenarios, comprising a series of attack steps, can be executed against the targeted infrastructure.

The execution of each attack step will generate a log or a trace that will be recorded.

Labeling of these records will yield a valuable dataset.

In the context of this specific problem, it is not possible to identify a de facto algorithm or approach to label data in this case.

In this work, we propose a hybrid approach that combines generated rules and anomaly detection.

The metadata from each attack step was then utilized to formulate detection rules that would identify traces associated with the execution of the attack step.

The events can then be associated with a specific attack step and technique and classified with a low false-positive rate.

Given that the execution of certain attack steps can generate multiple events, an anomaly detector module has been incorporated.

It has been demonstrated that events which do not share features of the attack steps can still be identified through this technique, thus reducing the false negative rate.

*Speaker