Beyond Gut Instincts: Understanding, Rating and Comparing Self-Learning IDSs

Markus Wurzenberger, Florian Skopik, Giuseppe Settanni, Roman Fiedler
Digital Safety and Security Department
AIT Austrian Institute of Technology, Vienna, Austria
firstname.lastname@ait.ac.at

***Abstract*—Today ICT networks are the economy's vital backbone. While their complexity continuously evolves, sophisticated and targeted cyber attacks such as Advanced Persistent Threats (APTs) become increasingly fatal for organizations. Numerous highly developed Intrusion Detection Systems (IDSs) promise to detect certain characteristics of APTs, but no mechanism which allows to rate, compare and evaluate them with respect to specific customer infrastructures is currently available. In this paper, we present *BÆSE*, a system which enables vendor independent and objective rating and comparison of IDSs based on small sets of customer network data.**

I. Outline

Actual reports [1], [2], [3] demonstrate that 77% of companies already have been affected by APTs and the remaining 23% are unaware that they could be. These sophisticated and tailored cyber attacks usually result in financial loss and tarnished reputation. There exist various solutions for IDSs, but currently there is no vendor independent and objective approach to analyse and evaluate them. Reasons for this are on the one hand the lack of data for testing. On the other hand security companies are not keen to share their secrets with potential competitors. The aim of our approach '*BÆSE* - Benchmarking and Analytic Evaluation of IDSs in Specified Environments' is to understand, rate and compare self-learning IDSs. This is a critical prerequisite for end-users to establish cyber situational awareness by using the most effective IDSs in their specific infrastructures. Additionally *BÆSE* also brings advantages for security solution providers.

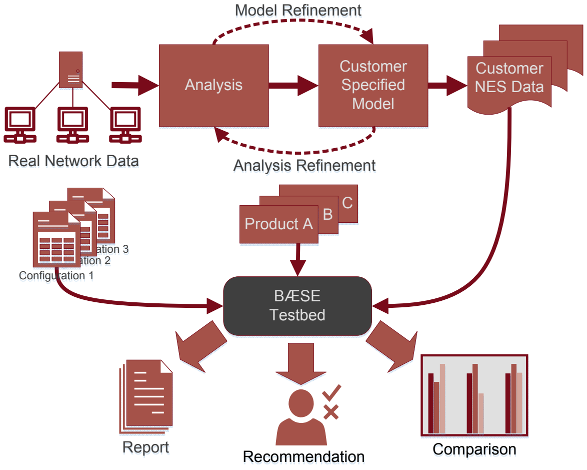

Figure 1. BÆSE concept and process phases

As shown in Figure 1, after extracting data from a real network, the next step foresees an accurate *Analysis* of the input data to characterise its properties. Then we calculate an instance of the *Customer Specified Model* to generate highly realistic customer *Network Event Sequence (NES) Data*, which serves as input for the *BÆSE Testbed*. For producing NES data of any different size, only a small set of real network data e.g., network packet traces or log data, is required. In order to enable scalable evaluation, ranging from quick to in-depth assessment, it is possible to iteratively and interactively refine the analysis and the model.

Automatically generated statistical reports and recommendations indicate the optimal IDS and the most effective configuration for user-specific infrastructures. *BÆSE* covers several security application areas, allowing security solution providers rating new products in network infrastructures of various size and shape, adapting existing products to specific customer requirements and estimating market potential of future IDSs. *BÆSE* can be employed for both (i) selecting the optimal security solution for a customer-specific network infrastructure by evaluating the most efficient configuration and (ii) rating the security mechanisms in place.

Preliminary assessment of the analysis and the modeling components show promising results, pointing out the effectiveness of our concept. Future work deals with the integration of the single components into a comprehensive system and in-depth evaluation.

Acknowledgements

This work was partly funded by the Austrian FFG research program KIRAS in course of the project CIIS (840842) and the European Union FP7 project ECOSSIAN (607577).

References

[1] AIRBUS Defence and Space, http://www.cybersecurity-airbusds.com/en_US/cybersecurity/advancedpersistentthreat-aptcheck/, 2015, Web - March 2015.

[2] Mandiant, "Threat report 2014. m-trends. beyond the breach." Mandiant, Tech. Rep., 2014.

[3] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security*. Springer, 2014, pp. 63–72.