Automating Threat-Intelligence Sharing

Alex Norta, Aleksandr Lenin and Anis Ben Othman
Department of Informatics
Tallinn University of Technology, Estonia
Email: alex.norta.phd@ieee.org, aleksandr.lenin@ttu.ee, anis.ben@gmail.com

***Abstract*—Security-operation centers (SOC) are a means to provide cheaper security services to companies so that the latter must not maintain their own costly security departments. In order to cut costs and time even more, several security providing companies share their security-threat intelligence (STI) and collaborate in meta-SOC creation. Thus, in a very selective way respective security providers share only subsets of their processes to protect specific STI and to also not disclose security-process details that constitute business secrets. On the other hand, the shared STI in a yields enhanced security-level measures. This paper fills a gap pertaining to suitable collaboration-model formalisms that permit privacy-assuring STI sharing. With the introduction of such a formalism, the foundation exist to automate meta-SOC management that currently relies on expensive human work.**

I. Introduction

II. Running Cases

III. Human Estimation Calculations

IV. Fuzzy Process Trees

V. Decisionpoint Metrics

VI. Feasibility Evaluation

VII. Conclusion

Acknowledgement