Dear editors,

Thank you for the opportunity to revise our paper, "Real-time processing of cybersecurity system data for attacker profiling", for publication in the proceedings from the *Informatics'2019 Conference*.

We would like to thank you and the reviewers for the very positive and constructive feedback, which helped us significantly improve the paper. We have gone through the comments very carefully and we have rewritten parts of the paper. In particular

- we specified in detail connection to previous research
- we have fixed quality of figures and
- we have proof-read and grammar-checked our paper.

The replies to the reviewers contain point-by-point responses to the specific comments in each review. Please do not hesitate to contact us if you need any additional information about the manuscript. Thank you for your consideration.

Kind regards,
Patrik Pekarcik

Reply to Reviewer 1

We would like to thank the reviewer for the comments which helped us a lot to improve the paper. In the following we address the comments in detail.

1. Comment: *Chapter III. Dataset (p.2): "We have split security data into three parts". Author(s) have to explain upon which criterions (i.e based on which) security data have been split.*

   Reply: *The entire dataset contained data over 4 weeks, the split was done based on the individual weeks. We corrected this information in the mentioned section.*

2. Comment: *Chapter IV. DESIGN AND IMPLEMENTATION OF A SYSTEM FOR REAL-TIME PROFILING, A. Implementation, It should read: "In our test environment which " instead of "witch".*

   Reply: *This typo was corrected. We also proof-read the paper for additional typos and checked the grammar.*

Reply to Reviewer 2

We would like to thank the reviewer for the comments which helped us a lot to improve the paper. In the following we address the comments in detail.

1. Comment: *The theoretical part of the paper should be blended clearly with the details of how it follows the research in [3]. For example, from the article it is not clear why exactly seven clusters are used, how they were formed or how the assignment to cluster was done. Moreover, the State-of-Art Section is more oriented to the clustering problems than to real-time processing of threats.*

   Reply: *We have specified in more detail how this paper follows the previous research in [3].*

   It is true that the State-of-the-Art section is oriented towards clustering methods, due to the fact they identify real-time processing for future work. In our ongoing research we aim to bridge that gap.

2. Comment: *The informative value of Figures 4 and 5 is not sufficient; a better description of the data in the Figures would be needed as well as their description in the text. For example, the paper says, "As can be seen in Fig. 4, the total number of IP addresses oscillates around a specific value", but on Fig. 4 no IP addresses are labeled.*

   Reply: *We have edited the description of both figures to make their information value clearer.*

3. Comment: *Also, it is not clear from the article whether the accuracy of the experiment has been verified.*

   Reply: *This paper reports current results of our ongoing research, where the verification methods are an identified research gap that we will address in our future work.*

4. Comment: *The weaknesses of the paper:*
   Weak explanation of the research it refers to.
   Deeper summary/conclusion is expected.
   Very low quality of Figure 2.

   Reply: *We addressed the first two weaknesses in the above comments.*
   Figures 1 and 2 were changed with a higher quality pictures.

5. Comment: *There is a typo: "a the second one was recalculating"*

Reply: *This typo was corrected. We also proof-read the paper for additional typos and checked the grammar.*