**Summary**

We believe the paper is well explained and structured, it could be improved and made a little bit stronger on the new metrics based on popularity. Our concern are explained in details can be found in the review report.

Our overall take on this paper is that there were way too many assumptions taken without any data backing. Which is fine but then it weren’t really explained or argued your point of view on the the assumption either.

**Strengths**

* We found that other than undermentioned issues, the strategies are strongly formed and reported.
* Data representation with Graphs and figures are quite clear.
* The paper is easy readable, the context in the introduction is bit weak which is explained in issues.
* Actors are well identified. But there are some issue in assumptions which can be found in following sections.

**Major issues**

* There were many assumptions made without the backing of any data. Such as:
  + It was mentioned “The problem owner is an actor which has the resources to tackle the problem.”
  + Also further it was explained that, Vendor is a problem owner and it is also rational to assume that the same organisation (vendor) also has sufficient knowledge and resources to research the problem.
  + We believe it’s not the case with every vendor. Every software creator do not have resources to research the problems. If we didn’t get it right? Then you defination need some direction to make the reader understand what you mean.
  + Another big assumption is the new metric based on popularity. The assumptions should be supported with logical explanations or research papers.
  + It’s being assumed that the more popular the software the less securer it gets and the vulnerabilities arise.
  + But in that case what we believe is that the software are still vulnerable enough but popularity motivates researchers and hacker to change their focus on them. For some obvious reasons like (more money, bigger bounties, more data etc.)
  + Though from the graph as a big picture it was also bit misleading. If you see the 2011 time chrome has more vulnerabilities but less users than the Opera.
  + But even if we don’t compare them with each other sure there is a rise and low not exactly parallel to popularity but closer.
* There are many assumptions taken in ROSI section. We have copied the snippets from your report for your refrence down bellow
  + Based on this figure decision-makers can view multiple scenarios for their security investment. A decision-maker can see what the expected impact is when he or she expects a 50 percent chance of occurrence
  + Of course, this figure is based on average data and the assumptions mentioned above. Therefore, it is important to take a further look at the probability of those figures, which will be addressed in the next paragraph.
  + Based on earlier analyses of the exploit rate of the vulnerabilities the ARO for the year 2015 is 12,9%. This leads to a Risk Exposure of 196,000 \* 0.129 = 25.284 US$
* **Weak examples:** deliver this as a service, like Symantec, they provide SSL-certificates that cover loss up to 1,500,000 US$ when the certificate is breached and damage has been done (Symantec, 2016) : SSL certification breech is a questionable offence
* “The impact of SQL-injections can also be reduced by performing output checks, such as limiting the amount of outputted results 4 from queries.” - how does the end customer use this solution? Would be better to have focussed examples.
* **Needs explanation:** You mentioned that risk acceptance similar to risk avoidance. It would be better to have an explained juxtaposition.

**Minor issues**

* Overall English was improved from last time, some minor grammatical issues and narration should be improved.
* Instead of using market share we will rely on the popularity of the software in its sector
* The only issue is that vulnerabilities tell us nothing about the level of security within an organization. And mainly the picture of number of vulnerabilities also doesn’t make sense much which we explained in details in Major issues section.