**Old Marketing Requirements**

1. Workflow must prioritize attack tools that are more likely to have  
   vulnerabilities.
2. Workflow must fuzz test attack tools for vulnerabilities.
3. Proof of concept program should mitigate or slow an attacking tool
4. Proof of concept program should provide an active defense response
5. Proof of concept should show that the workflow functions
6. Proof of concept should use AI/LLM to generate responses capable of  
   neutralizing or slowing the attacking application
7. Findings should be placed into an IEEE/ACM style paper

**Revised Marketing Requirements**

1. Workflow must prioritize attack tools that are more likely to have vulnerabilities.
2. Two selected attack tools to test against must be identified.
3. Software fuzzing tools capable of testing both attack tools must be identified.
4. Demonstrate a fuzz testing workflow for selected attack tools Medusa and Masscan.
5. Proof of concept should show that the workflow functions.
6. Proof of concept program must provide an active defense response.
7. Proof of concept must use AI/LLM to generate responses capable of neutralizing or slowing the attacking application.
8. Evaluate the performance of any active defense responses found.
9. Findings must be compiled into an IEEE/ACM-styled paper.