Application security without rose-colored glasses

From perspective of an infosecurity community member

How we see software development

How we see software developers

How we think we work together

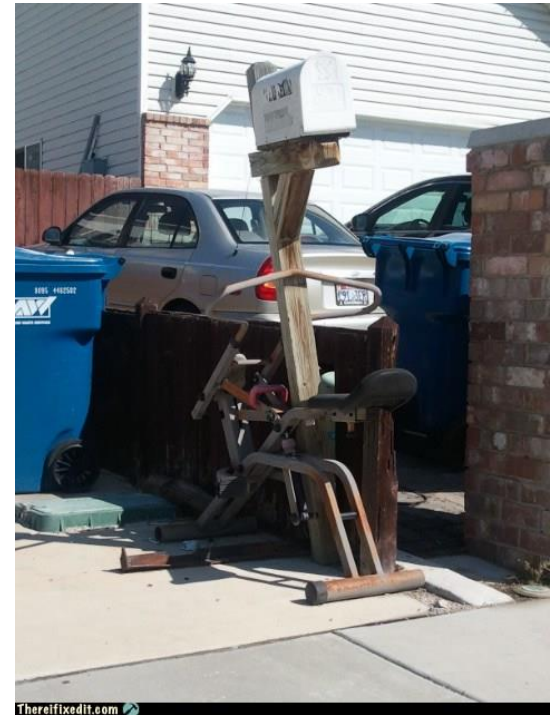# How we think security controls are implemented

But in reality it looks different…

In reality software looks more like this

How software is maintained

How we see ourselves

How we feel they see us

How they really see us

How we see policies

How they see policies

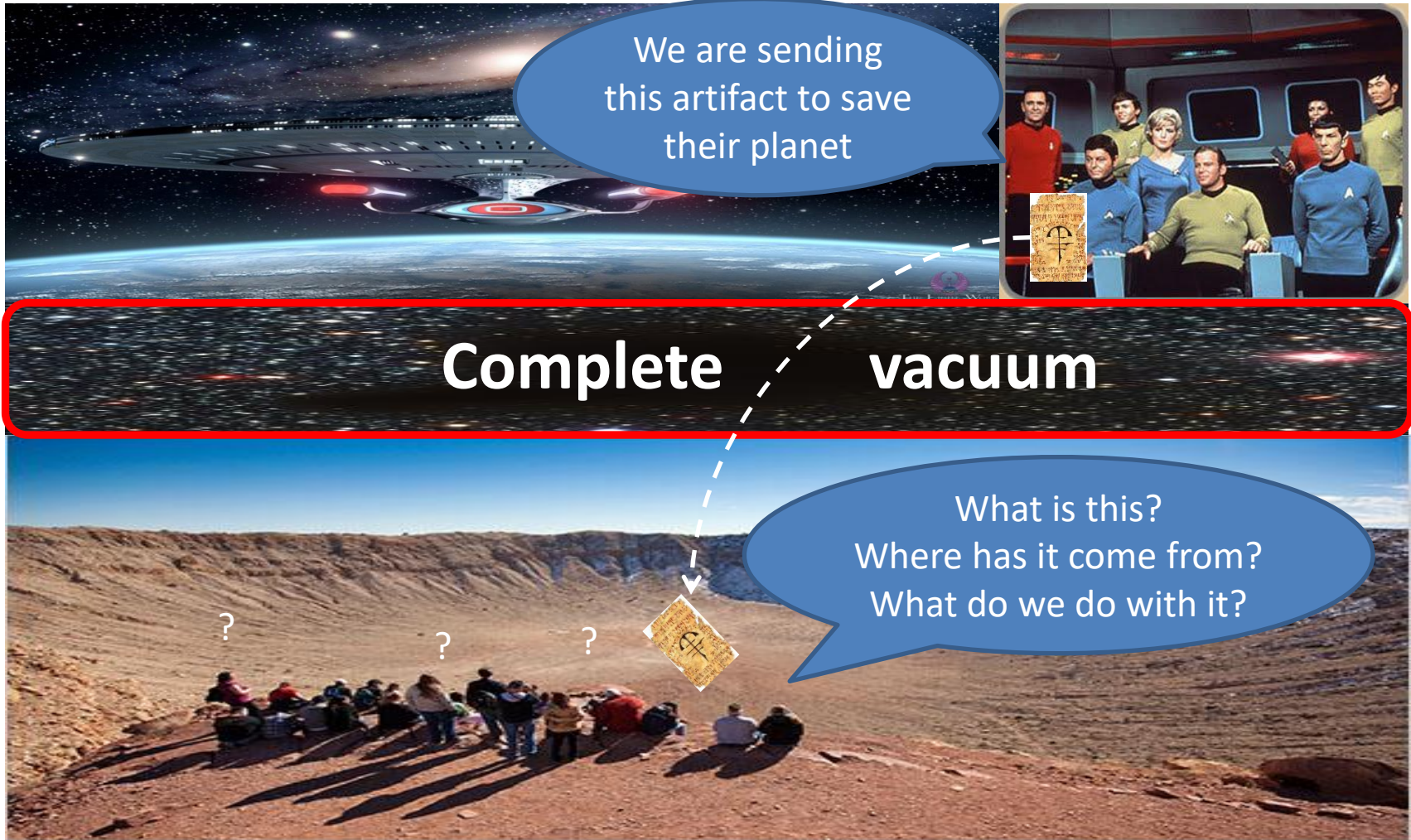# How they see our initiatives

What we get in the end

Where this leads to

Why is this happening?

#1. Communication vacuum

#2. No balance between the desired result and effort needed to be spent in order to achieve it
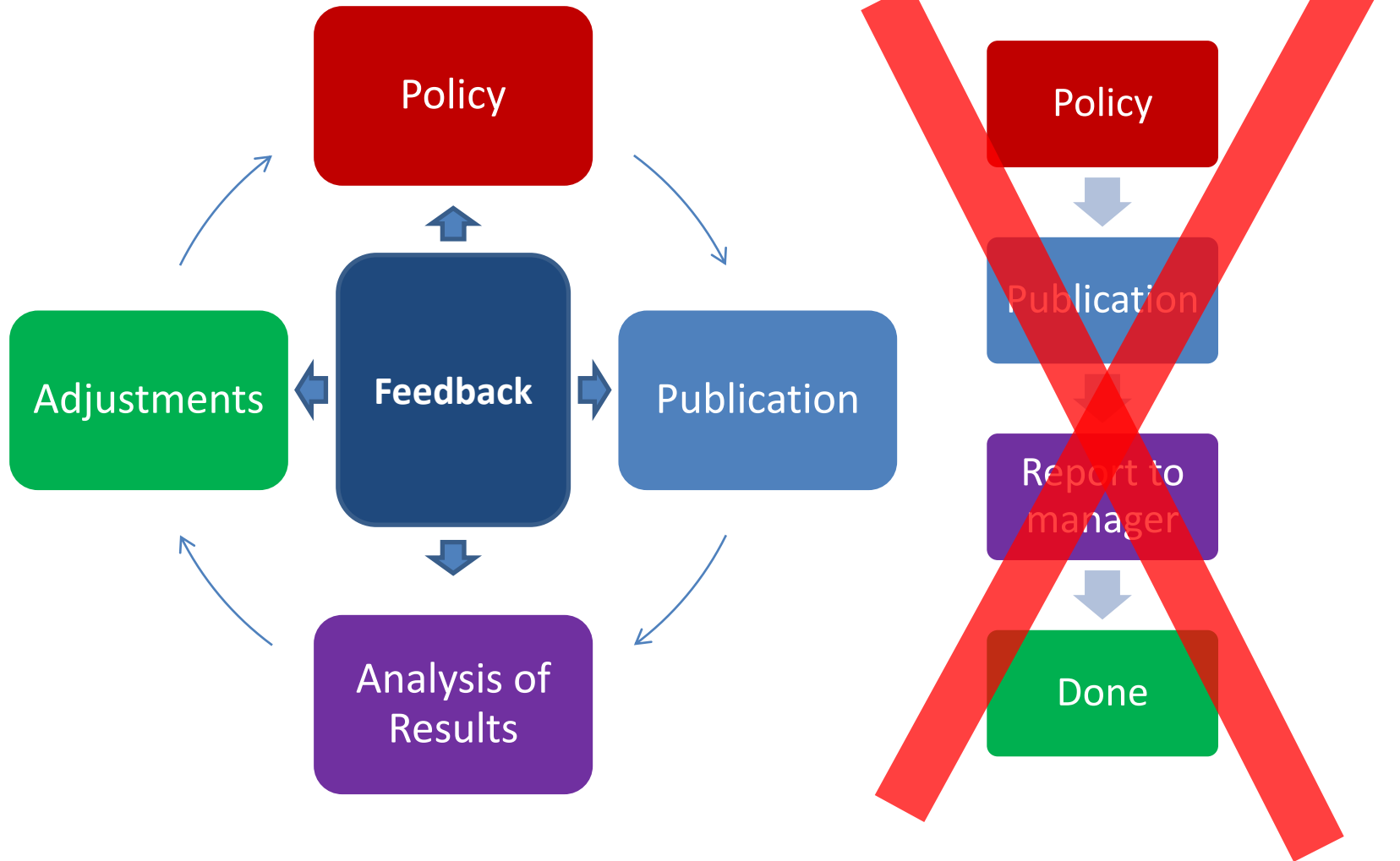
How to fix this?

Communication is the key

1. Eliminate vacuum in communications
2. Get closer to target audience, talk to them, get their feedback
3. Work together to ensure that the target is realistic to achieve and all necessary tools and resources are available
4. Find balance between desired result and effort spent to achieve it – otherwise there will be no result at all
5. Don't stop when agreement is made and artifacts are produced. This is only the beginning
6. Continuously analyze results of your work and try to find sources of any issues, adjust accordingly

Policy maintenance is a continuous process

P.S.

How they see me

How I see myself

Contact me:

mikhail@samoylenko.me