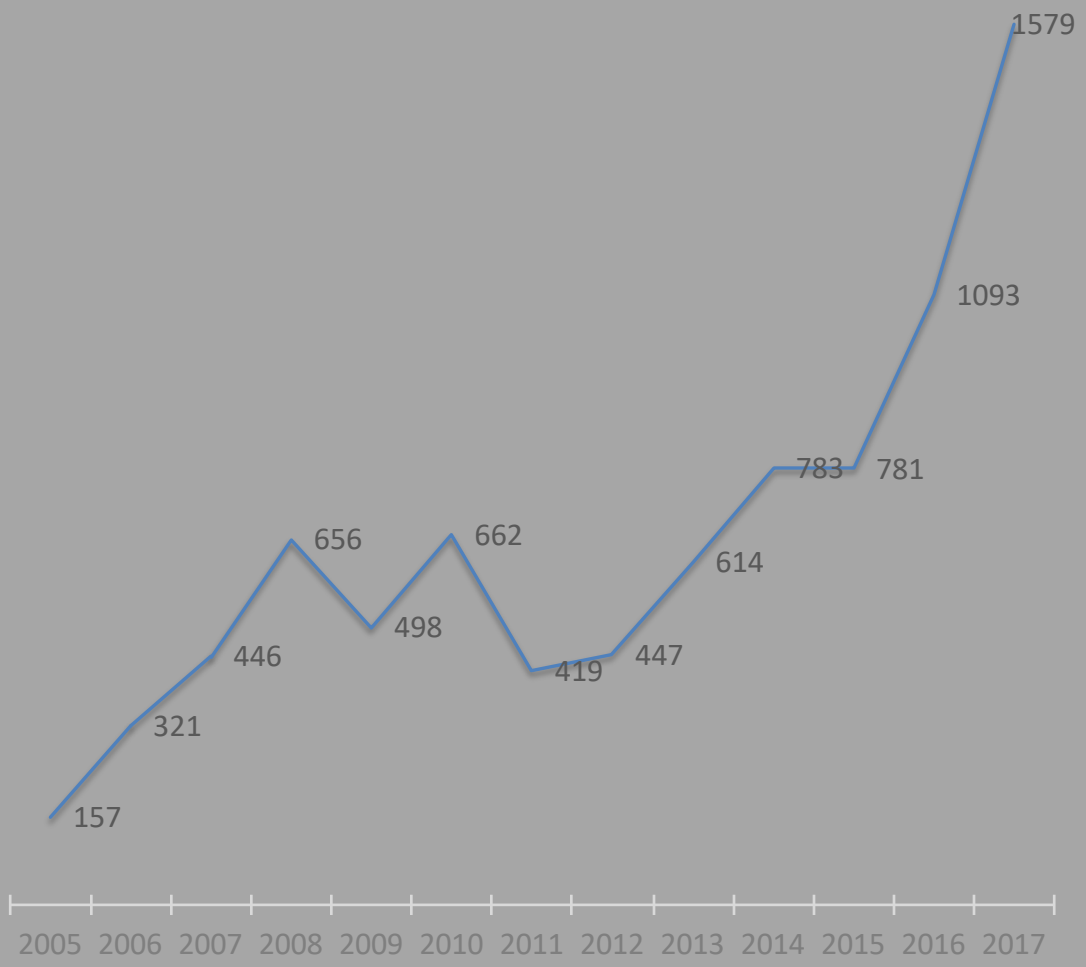
Creating the Attacker's Dilemma

Tim Crothers, Vice President Cyber Security, Target Corporation

“Defender’s Dilemma”

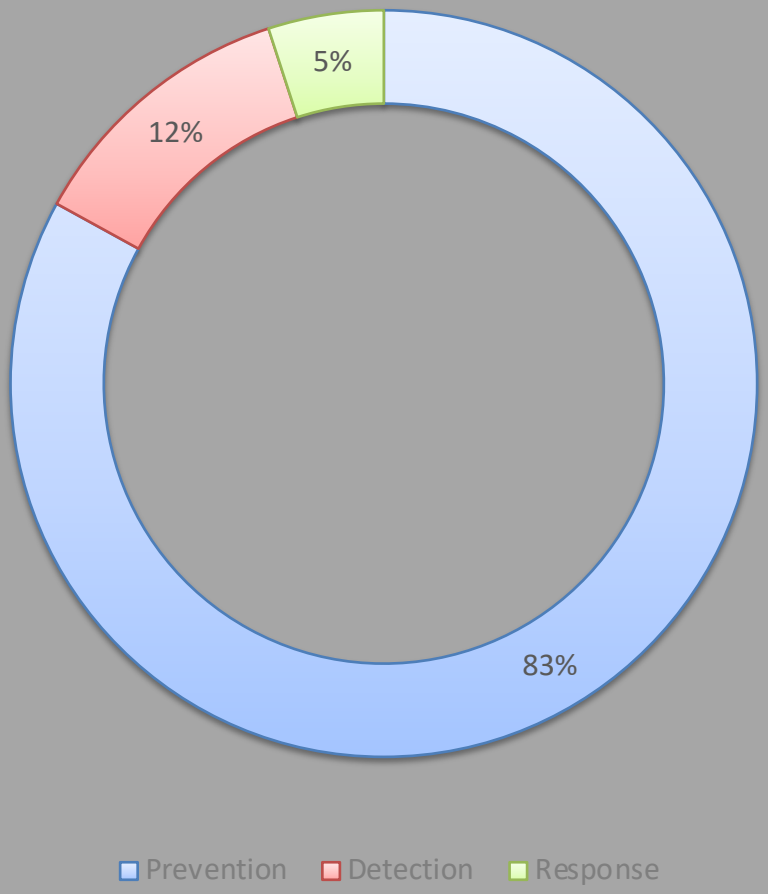
“Breaches are inevitable because the defenders have to be right 100% of the time whereas the attackers only have to be right once.”



Data Breach Statistics

Despite ever increasing information security spend and regulatory requirements the problem is growing worse not better.

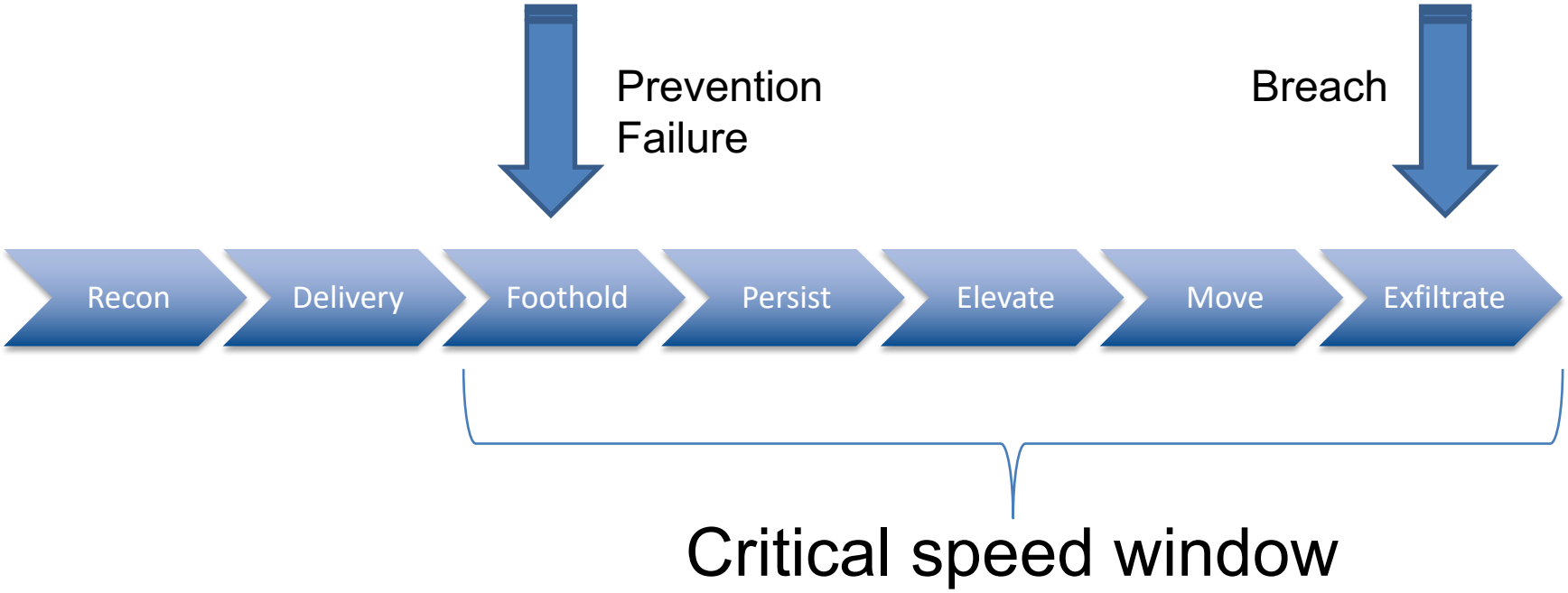
Is Cyber Security a Technical / Tool Problem or a People Problem?

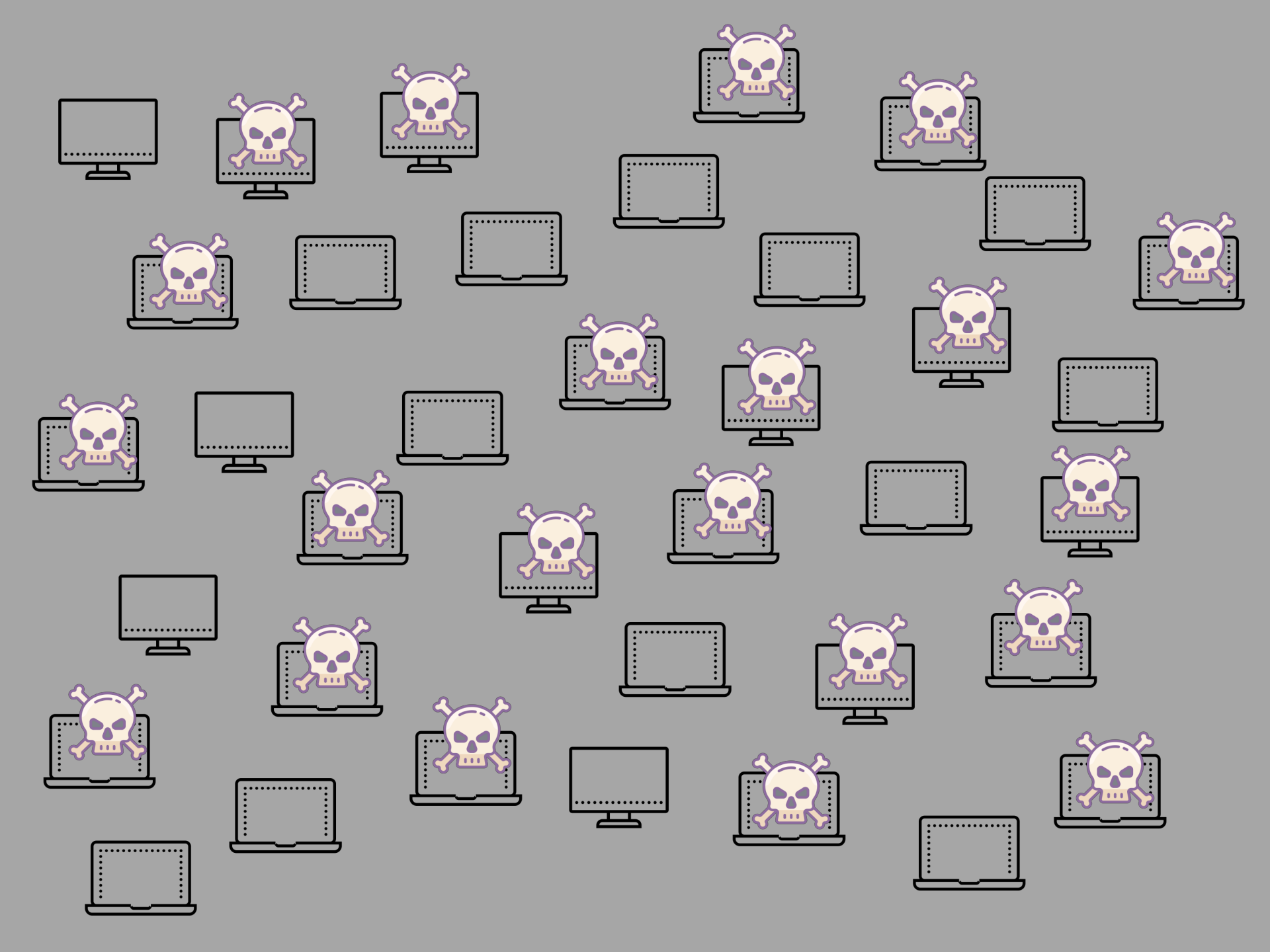


Organizational Information Security Spend.

Most institutions are heavily indexed on preventative technologies. The proper ratio is different for every entity but over-indexing on prevention leaves insufficient ability to know when prevention has failed and respond accordingly.

When does a “Breach” occur?





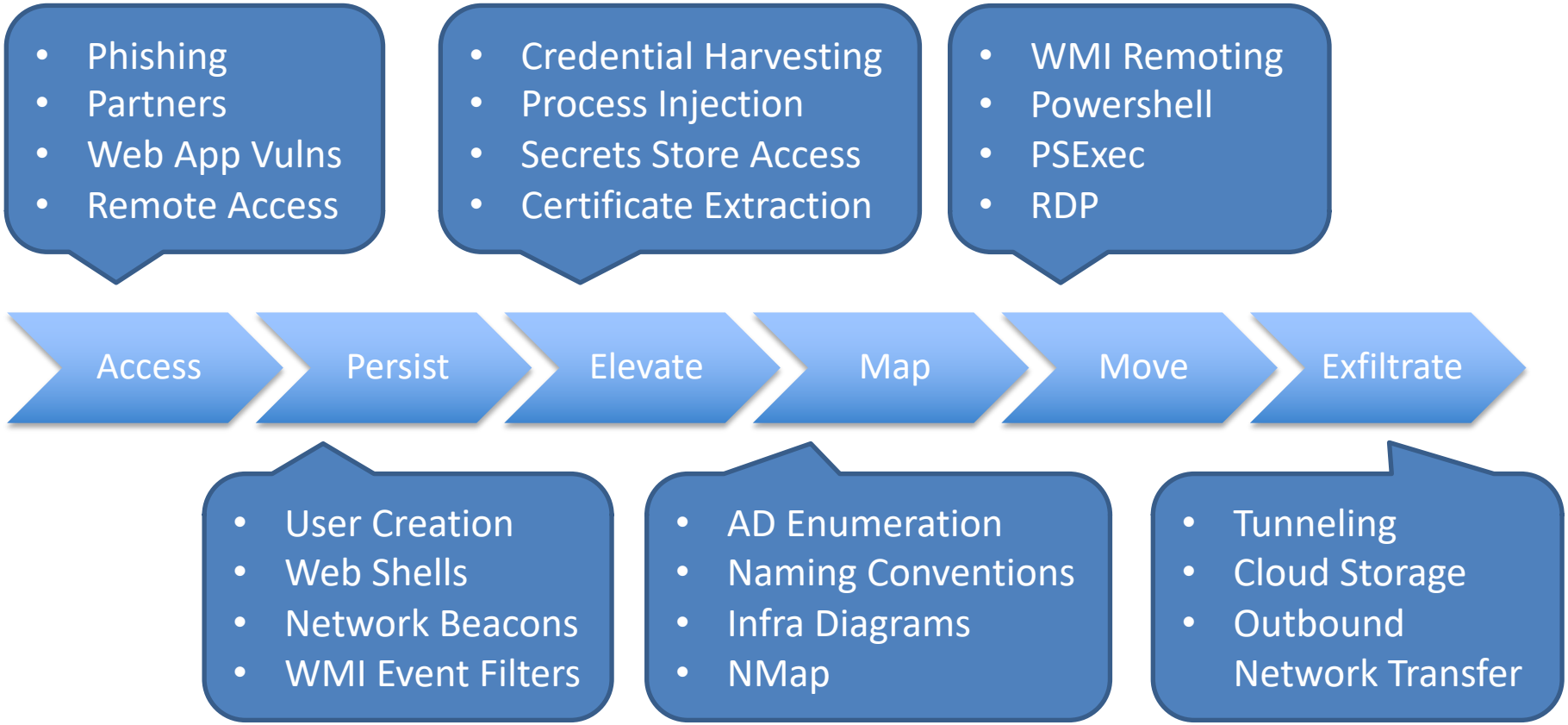
“Attacker’s Dilemma”

How do they get to their goal and exfiltrate their stolen data without tripping a single one of our detection ‘landmines’?

Creating an Attacker's Dilemma

1. Focus on the criminal's activities rather than the tools and exploits
2. Use the attacker's needs and techniques against them
3. Balance prevention, detection, and response appropriately
4. Invest in your people over your tools

Needs of the Attackers…



Using the Attacker's Needs…

- Lure accounts for cached credential scraping
- Fake accounts to use to respond to phishing waves
- Lure credentials on open Github repositories
- Fake data posted on internal wiki's
- …

Balance…

Prevention is extremely effective at stopping a LOT of attacks…

… something like 99.9+%

Unfortunately prevention is just a speed bump for the actors responsible for most of the breaches…

… almost all of the hospitality and retail food industry breaches in 2016 and 2017 were due to a single group…

Determine the RIGHT level of prevention for your organization and then focus the remaining resources on detection and response

Invest in your People…

People can out think other people (i.e. criminals) whereas tools can't…

When properly inspired people are endlessly inventive…

When properly skilled people are able to outperform tools…

Tools are rigid, good people are not…

People can adapt to rapidly changing situations and tools can't…

Homework

1. What is the ratio of your information security spend when categorized between prevention, detection, and response?
2. When you “lift the hood” of your detection is it looking for the behaviors of the criminals or the tools used by the criminals?
3. When you look at your SOC alerts how many of them are indications that you have a prevention failure or just evidence your prevention is doing its job?
4. How quickly are you containing “prevention failures”?

Thank You!

 @soinull

 linkedin.com/in/tim-crothers-5458738/

 https://github.com/soinull/Attackers_Dilemma