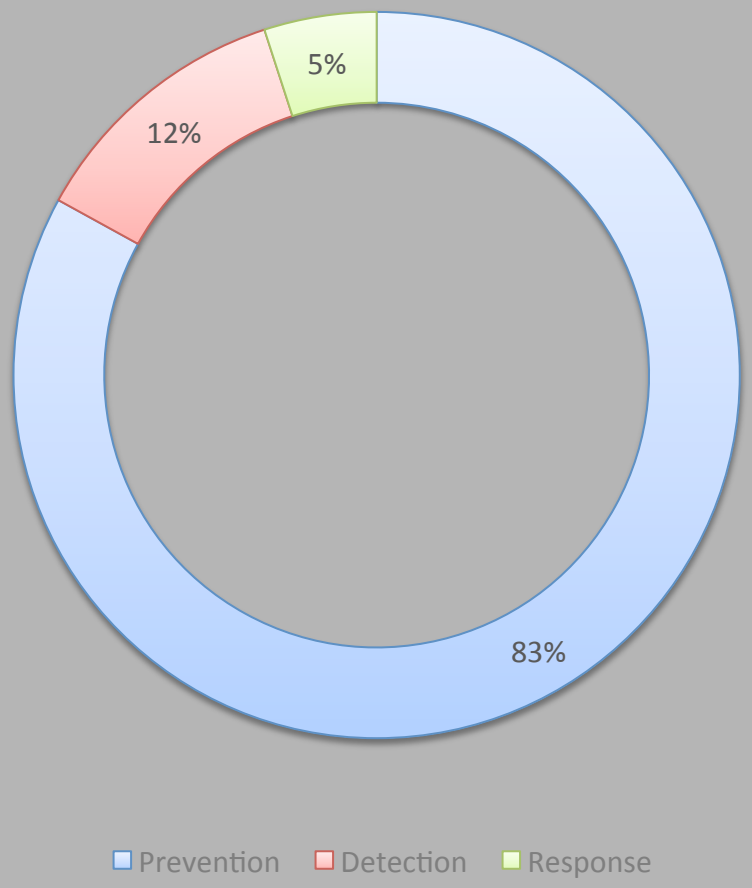
Using Deception Techniques to Create Strong Detection

Tim Crothers, Vice President Cyber Security, Target Corporation

“Defender’s Dilemma”

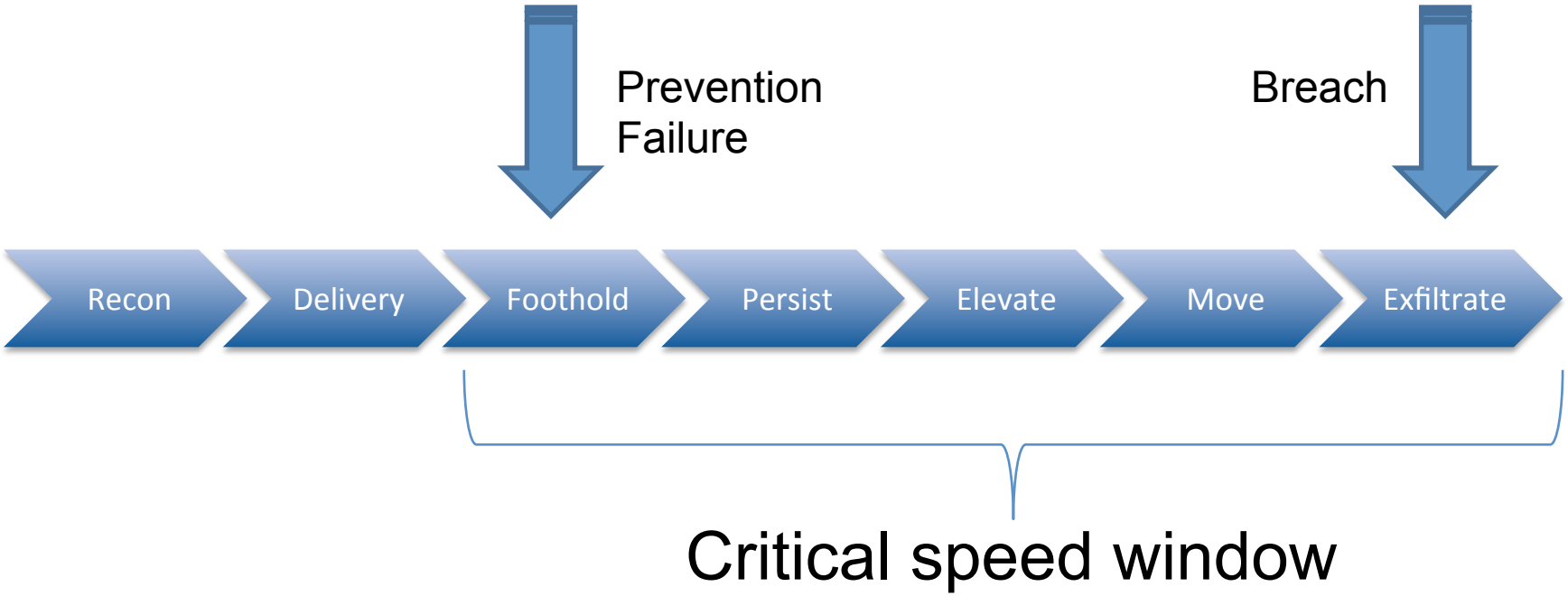
“Breaches are inevitable because the defenders have to be right 100% of the time whereas the attackers only have to be right once.”



Organizational Information Security Spend.

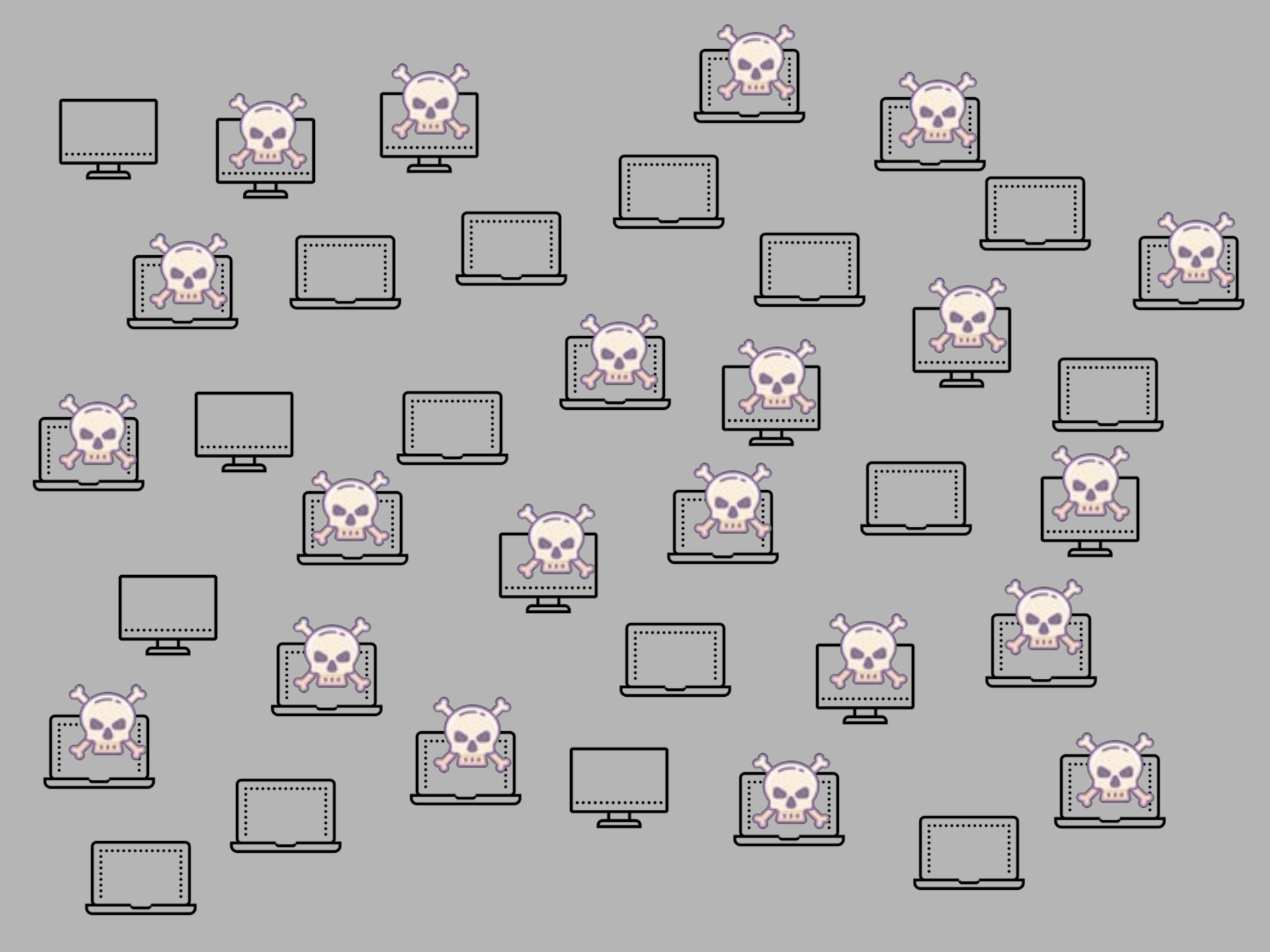
Most institutions are heavily indexed on preventative technologies. The proper ratio is different for every entity but over-indexing on prevention leaves insufficient ability to know when prevention has failed and respond accordingly.

When does a “Breach” occur?



“Attacker’s Dilemma”

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



Weaponizing our endpoints

1. **Plan out the lures for maximum authenticity**
   1. ID's should follow organizational standards
   2. Consider which endpoints to add lure caches to and which not to
   3. Consider whether just some endpoints (and which) should have local secrets cached
2. **Create lure domain accounts**
3. **Log in locally on end points with lure domains to cache them locally**
4. **Add local secrets credentials to strengthen lures**
5. **Change lure domain account passwords**
6. **Implement alerting on attempted use of our lure accounts**

Thank You!

 @soinull

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

 https://github.com/soinull/Strong_Detection

https://github.com/soinull/Weaponizing_Endpoints