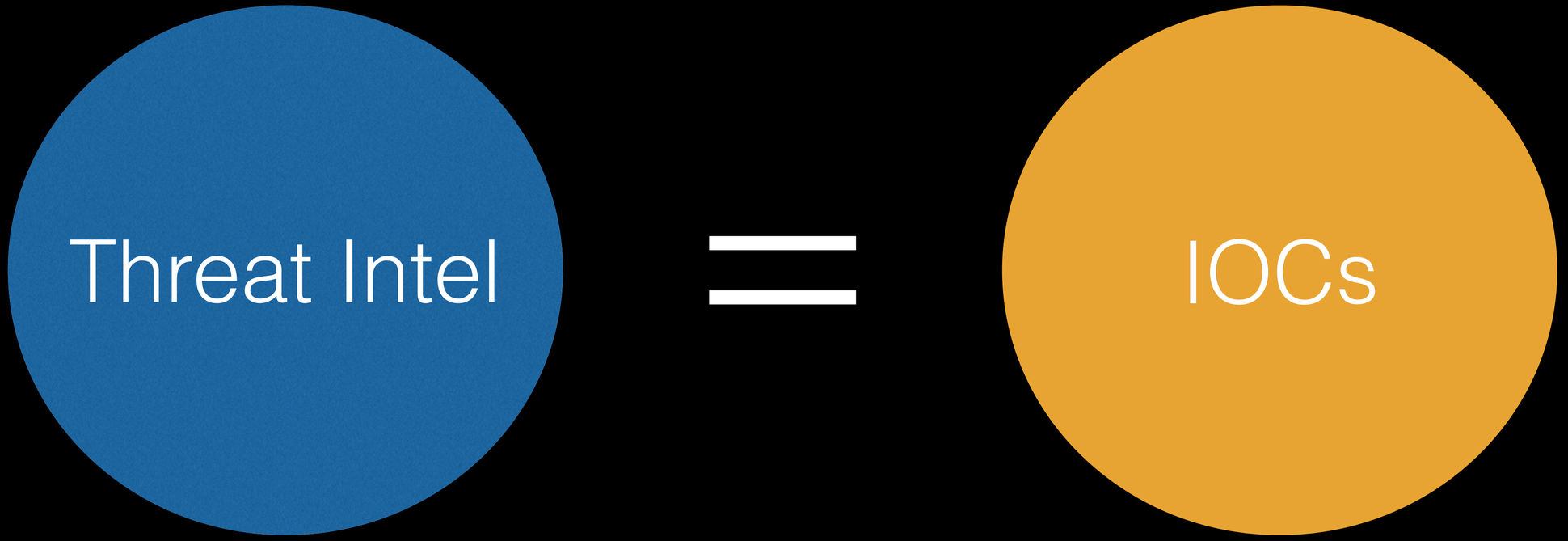
IOC sharing - we are doing it wrong

Csaba Fitzl, BSidesBUD 2017.03.02.



Common interpretation

Noooooooooooooooooo!!!!!!!!!!!!

Reality

IOC Madness

- Everyone wants to consume IOCs
- Some people wants to share
- Open Source IOC feeds

Sharing - IOC types

- Huge number of IOC types
  - being shared: hash, domain, URL, IP, filename
  - but what about: registry, filemods, processes, mutex, etc…?

Sharing format

- Typical: TXT (email, website); PDF - that itself would worth a punishment!
- CSV should be the bare minimum
- STIX/TAXII, OpenIOC would be the right way

Sharing hash type

- Vendors share MD5
  - or SHA256
  - Typically not the two together
- Why is it a problem?
  - MD5 collisions
  - Some security tools can search MD5 some SHA256, but not both.
- Workaround: try to find the sample on VT

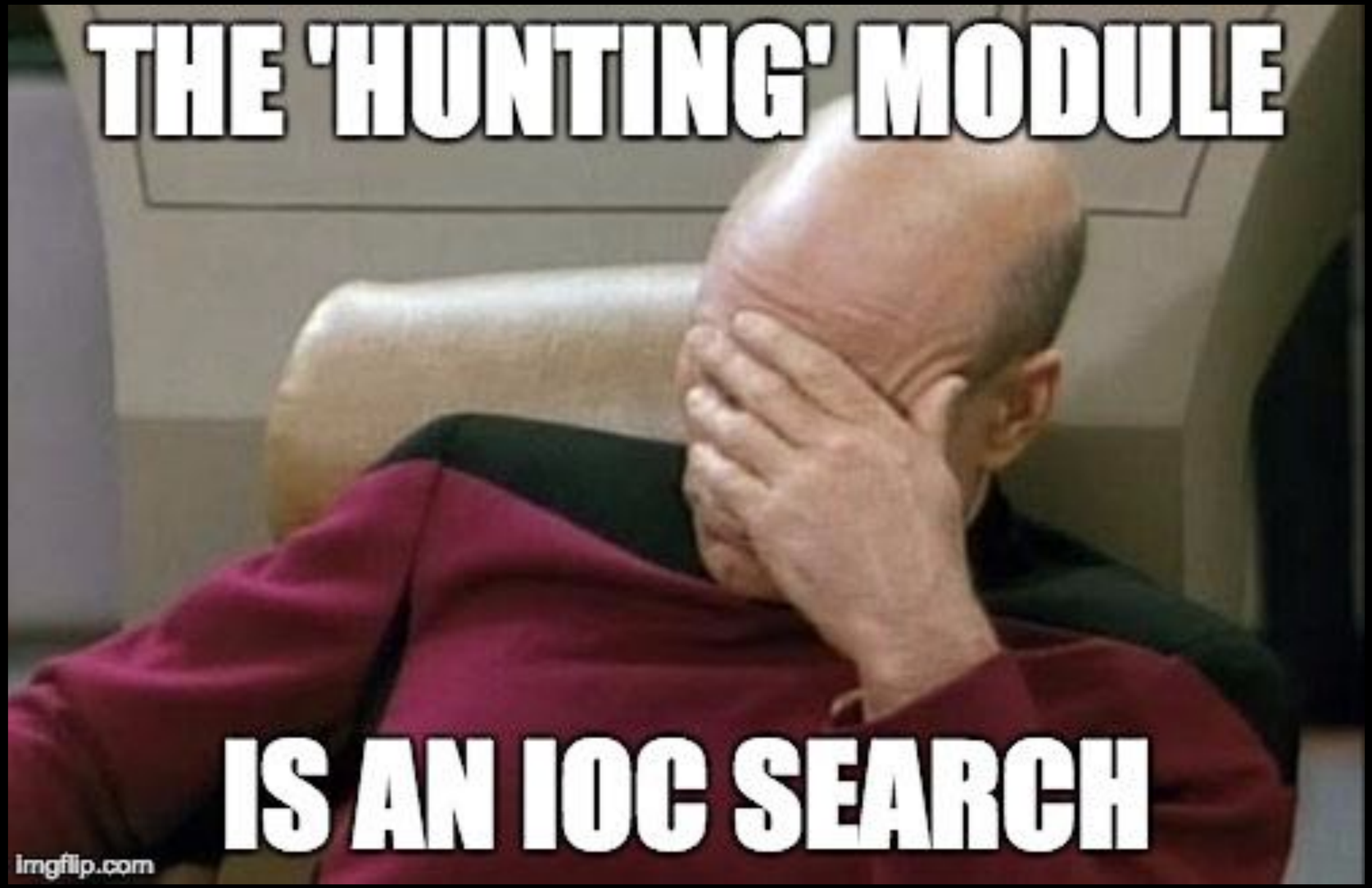
Usefulness

- Hash - Few hashes compared to half million new hash/day - really??
- IP - Think when one IP shares 100+ websites/domains, and some of those popular - how many FP?
- Filename - Somewhat better than hash
- Domain - Probably the best and most useful one

Summary

- IOCs have their place in IR
  - but they won’t save the world
  - should be treated properly

The Problem begins when…



What I would like to see?

- Please share SHA-1, SHA-256, SSDEEP hashes as well beside MD5 (share all 3 not just 1 of them)
- Please summarize other IOC information as well - especially behavioural type of info, not just IP, domain, filenames and hashes
- Please share IOCs in STIX / OpenIOC format but at a minimum in a CSV

?