The Future of Global Vulnerability Identification and Reporting

November 28, 2011

Initial Discussion at ITSAC – Nov 2nd

The issues we must be concerned about in global vulnerability and identification include:

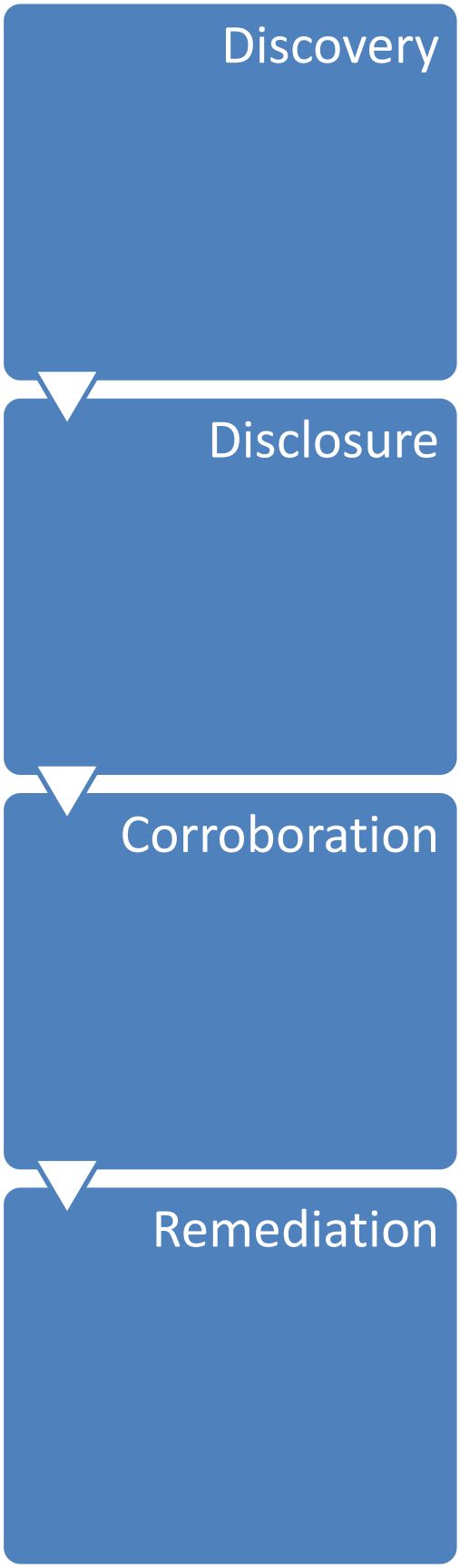
- Coverage
- Timeliness/Speed
- Counting Accuracy (granularity)
- Findability
- Level of Abstraction/Uniqueness
- Process Integrity
- Data models

Maybe Two Namespaces?

- One for “promiscuously”-assigned standard vulnerability identifiers (*VID*’s)
  - Many existing schemes: XF, Secunia, BugTraq, etc.
  - Anyone can generate - *fast*
  - No guarantee of correctness, uniqueness, etc.
  - Lightweight
- One for *CVE-type* identifiers
  - Requires significant analysis
  - De-conflicted, de-duped
  - Necessary before many will act

CHATHAM HOUSE RULE BTW

This meeting is being held under the Chatham House Rule.


Discovery
Disclosure
Corroboration
Remediation

Does this make sense?

Cve.mitre.org:2011-0175

Holes-in-mumps.tv:2011-0188

Kb.cert.org:2011-375689

Mozilla.org:##### etc

?

Suggested Focus for (some of) Today

- Explore the “VID” namespace issues
  - Purpose
  - Format
  - Data model
  - Relationship to “CVE-type” ID’s
  - Registries
  - …

Next Steps

- Suggestions for tackling the “CVE” part of the problem