# Introduction to CRF


"Common Result Format"

MITRE

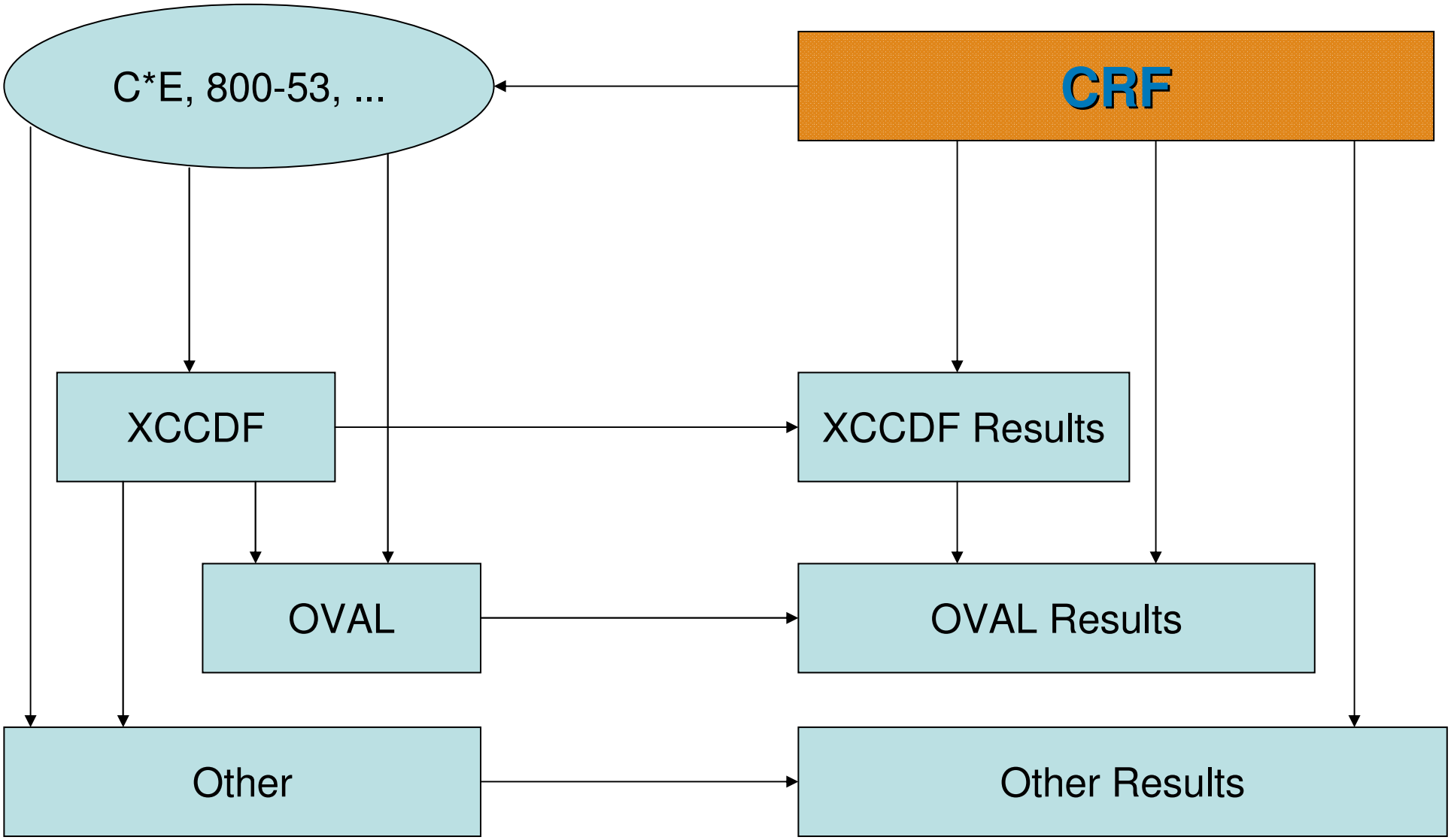
# What is CRF?

- inclusive standardized assessment result format
- result aggregation across the enterprise
- based on common names
- allows references to low level checking data
  - checks, parameters, and results

# Some examples...

- How many assets have CVE-2007-1234?
- How many assets have Office 2003 installed?
- Which systems are out of compliance?
- What is my compliance score?
- How has an asset changed over time?

# Where does CRF fit?

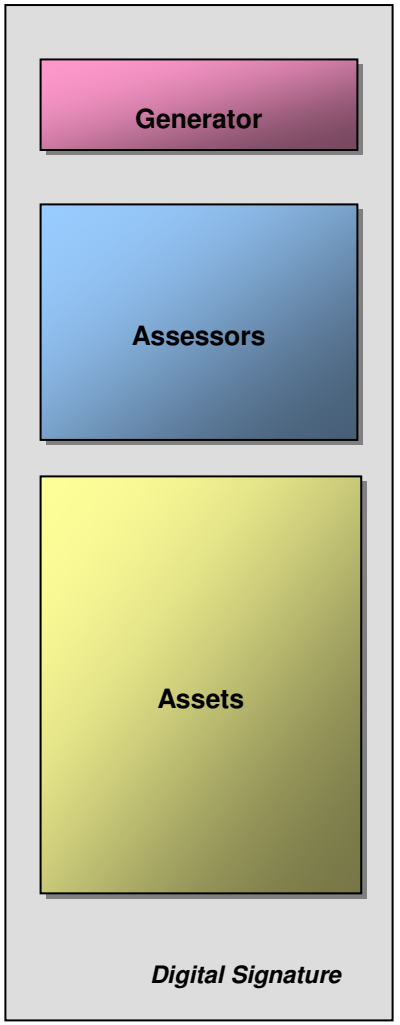


# Key points...

- if the tools in your enterprise can report findings based on common names then you can use CRF
- roll up of data in heterogeneous environments to gain the most complete picture
- aggregate assessment data across tools
  - patch management system
  - vulnerability scanner
- findings are based on well known names
- an asset can be represented multiple times
  - scanned by several tools
  - scanned several times by the same tool
- motivate vendors to use common names

# CRF Structure

- Generator
  - What app created the doc & when
- Assessors
  - Which tools did the assessments
- Assets
  - LCD approach to asset identification
  - A set of findings



# Current Status

- in early draft form
  - an update will be posted next week
- soliciting feedback now
  - we want your input
- future revisions will
  - formalize versioning
  - formalize community
  - develop use cases
- Review the spec and schema at: http://crf.mitre.org