Analytical Tool Evaluation Framework

Timothy Shimeall, Ph.D.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Outline

Analytical Evaluation Framework

Updated Evaluations Process

Data Evaluations

Indicator Evaluations

Analytical Evaluation Framework

Systematic & objective process of evaluating possible components of a security analysis process and determining their place of utility

- Focused, not restricted, traffic analysis processes
- Input, process, output
- Levels of abstraction, maturity, completeness
- Gaps and value add

Phase I (last year): detailed table-driven characterization; nouns/verbs/adverbs/adjectives

Phase II (this year): specific and actionable points from evaluation; agile evaluation; variable applicaton

Updated Evaluations Process

Previous work products too slow, long, detailed

- Too academic an approach: taxonomy, scoring, averaging
- Results not actionable

Targeted information:

- Functional overview
- Area of applicability
- Strengths and weaknesses
- Limitations and remediation
- Gaps
- Costs & requirements
- Role in analysis process

Structured process to produce rapid turnaround reports with value added

Several tool evaluations performed

Roll-up report summarizing differences in similar tools

Data Evaluations

Multiple possible data sources

Evaluating data as process component:

- Content
- Source
- Format / access method
- Strengths / use cases
- Restrictions
- Issues / remediation
- Validation / reliability
- Requirements
- Role in analysis process

Multiple evaluations performed

Roll-up report documenting commonalities, supplementary aspects, redundancies

Indicator Evaluations

Indicators over multiple data, multiple sources

Characterize indicators to facilitate comparison

- Functional description
- Relative strengths and weaknesses
- Use cases / threat coverage
- Limitations and restrictions / remediation
- Timeliness, validation, reliability
- Role in analysis process

Ongoing activity

Roll-up across indicators planned

Conclusions

Evaluation framework still based in formal support

Agile evaluation process

Targeted evaluation results

Diversified from program (tool) evaluation to process component evaluation

Ongoing development