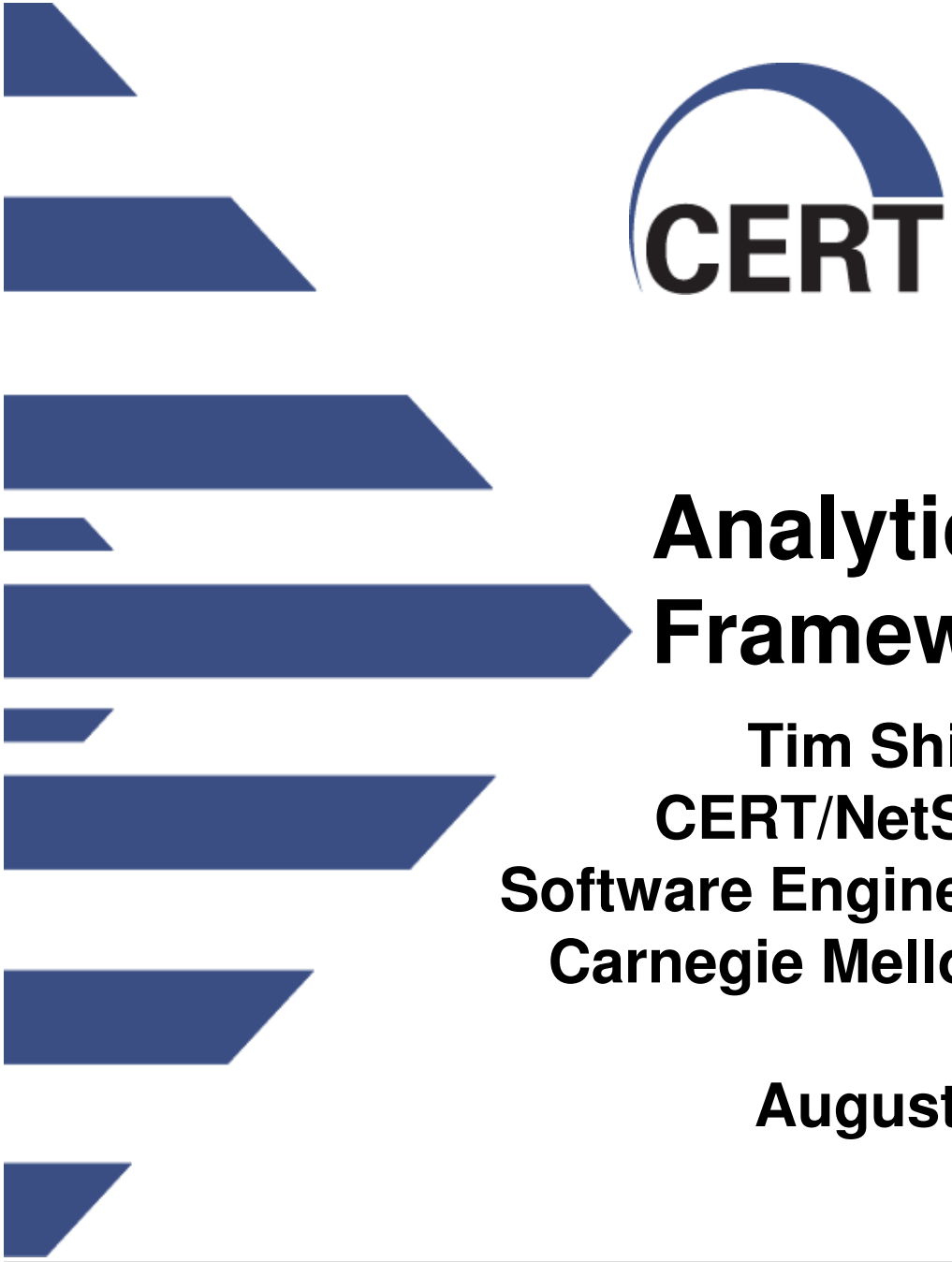


Analytical Evaluation Framework

Tim Shimeall
CERT/NetSA Group
Software Engineering Institute
Carnegie Mellon University

August 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Analytical Evaluation Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
GFIRST 2011: 7th Annual Government Forum for Incident Response and Security Teams (GFIRST) National Conference, 7-12 Aug 2011, Nashville, TN.

14. ABSTRACT
This presentation provides a framework for evaluating network traffic analysis tools.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**17**	

Disclaimer

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.

Describing Network Analytical Capabilities

Develop descriptions that support fair evaluation of current or potential capabilities to address network defense needs and operational cycles

- "How does it fit" not "Is it good"
- Input to acquisition, not decision for them
- Methodical and impartial, not objective

Supportive of network security, but applicable somewhat beyond just network security

- Harvest analyst expertise
- Consideration of carry-over effects

Phase 1: A Language Model

Nouns – forms of data handled by the capability

- Inputs
- Processing
- Results

Verbs – primitive actions supported by the capability

- Data handling
- Process
- Analytic
- Presentational

Adverbs – characteristics of the capability

- Process
- Product

Prepositions – scope or limitations of the capability

Assessing Data

What is the primary data handled by the capability?

What is secondary data handled by the capability?

What is supportive data handled by the capability?

What primitive operations are associated with each?

How well are the operations implemented? What is missing?

Example: Sourcefire IDS

Primary input: Packet data

- Collect, Abstract, Parse, Alert, Store, Query, Export

Secondary input: Network map

- Select, Group, Aggregate

Supportive input: Signatures

- Import, Alert, Store, Export

Input/Processing/Output

Input: what data does the capability consume?

- Sourcefire consumes network packets

Process: what data is used for control or direction of the capability?

- Sourcefire uses signatures and network configuration information

Output: what data is produced by the capability?

- Sourcefire produces alerts, and selective packet capture

Network Level of Abstraction

Many capabilities are focused on particular range of protocols and behaviors

- IP layer: packet-based analysis, does not get into local behavior and only infers application behavior (e.g., SiLK)
- Application layer: message-based analysis, does not deal with transport mechanics (e.g., analysis of email patterns)

Assessing Operations

What locus of operations forms the “core” functionality of the capability?

What are secondary operations?

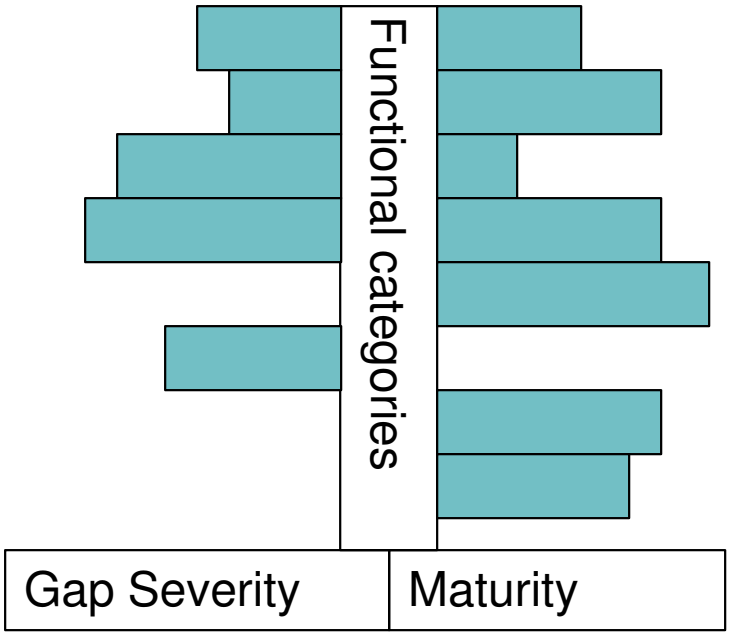
What are supportive operations?

How well are those operations implemented?

How scoped is the intended application?

Rating scheme: 0-5, plus n/a, not eval, absent

Summarizing Operational Gaps/Maturity



- Balance functional maturity vs. capability gaps
- All tools have gaps
- Goal is to see how peaks and valleys match

Process Adverbs

Sourcefire IDS:

Operational

Qualitiative

Tactical

Concise

Product Adverbs

Sourcefire IDS:

- Not Data-diverse
- Immediate
- Responsive
- Interoperable
- Documented
- Supported
- Trained
- Robust
- No Workflow
- No AAA

Prepositions

Under Conditions (e.g., edge vs. transit)

At Size / scale (e.g., enclave vs. enterprise, days vs. months)

Of Scope (e.g., CND vs. network ops)

Within Coverage (e.g., sparse vs. complete)

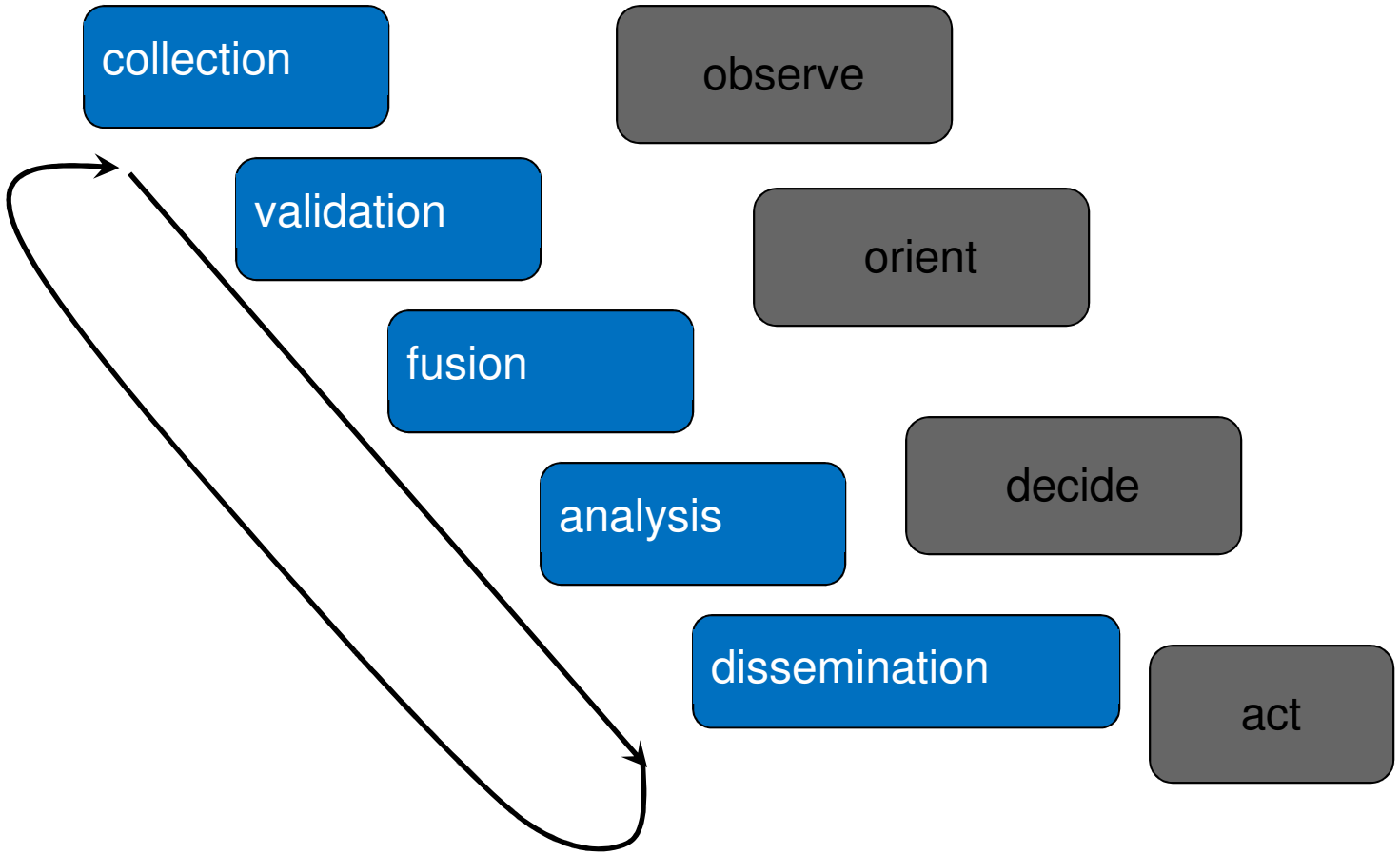
In time (e.g., interactive vs. batch vs. continuous)

Phase 2: Process Descriptions

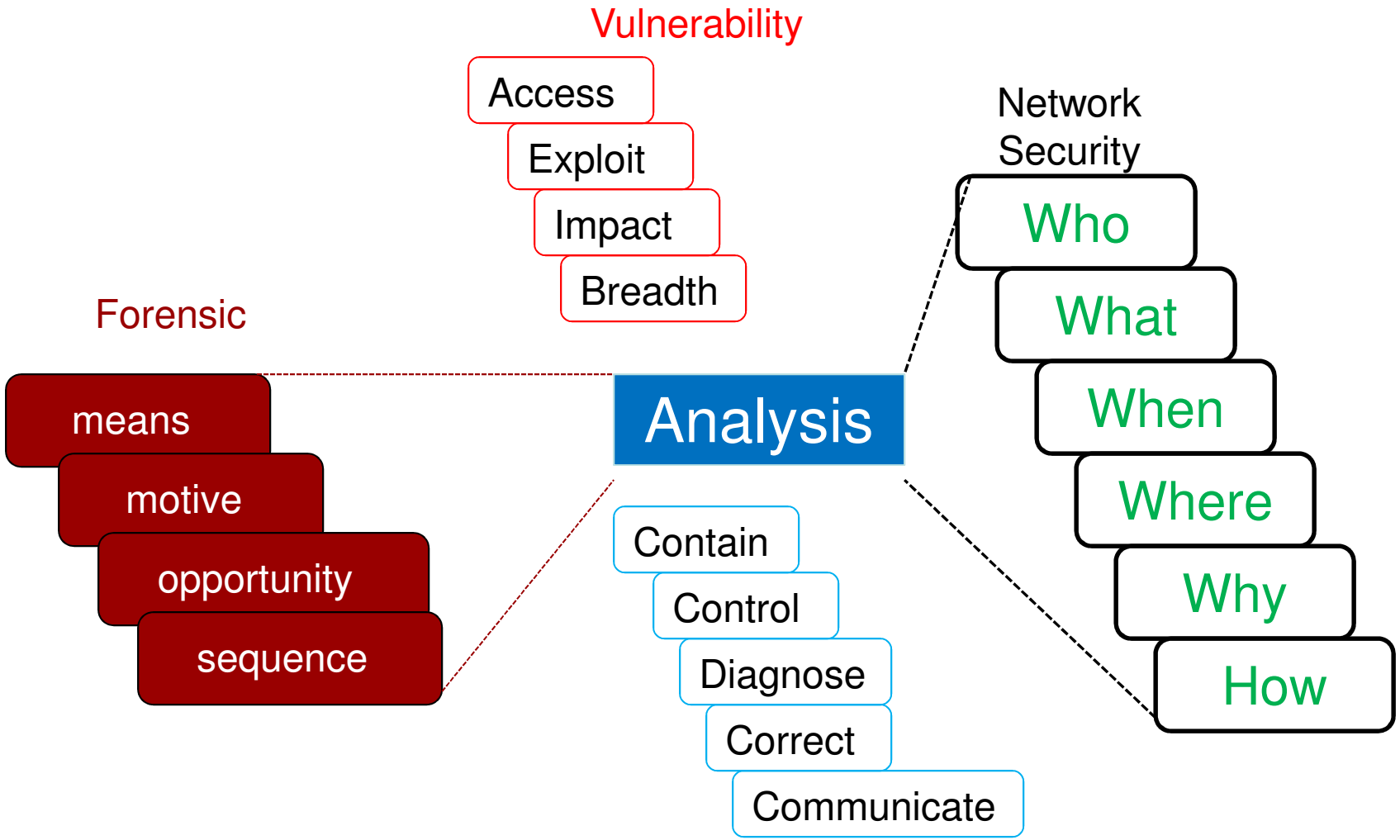
What form of reasoning should the model support?

- Fused-source intelligence
- C2/OODA?
- Forensic?
- Bayesian hypothesis testing?
- Abductive pattern matching?

Network Analysis Approaches



Analysis Decomposed



Next Steps

Expand initial visual results into fair comparisons

- Spider diagrams
- Input/Process/Output tables
- Network level tables
- Operational maturity/gaps

Define requirements for evaluation process using model

- Team?
- Approach?
- Process?
- Outcomes?
- Threats?

Tie capabilities to process needs

- Threshold approach (score needs to be X)
- Conditional approach (capability must include Y)
- Descriptive approach (need to support operations Z)

Reasoning Support