SATE VI Background

Vadim Okun
National Institute of Standards and Technology
19 September, 2019

https://samate.nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cautions on Using SATE Data

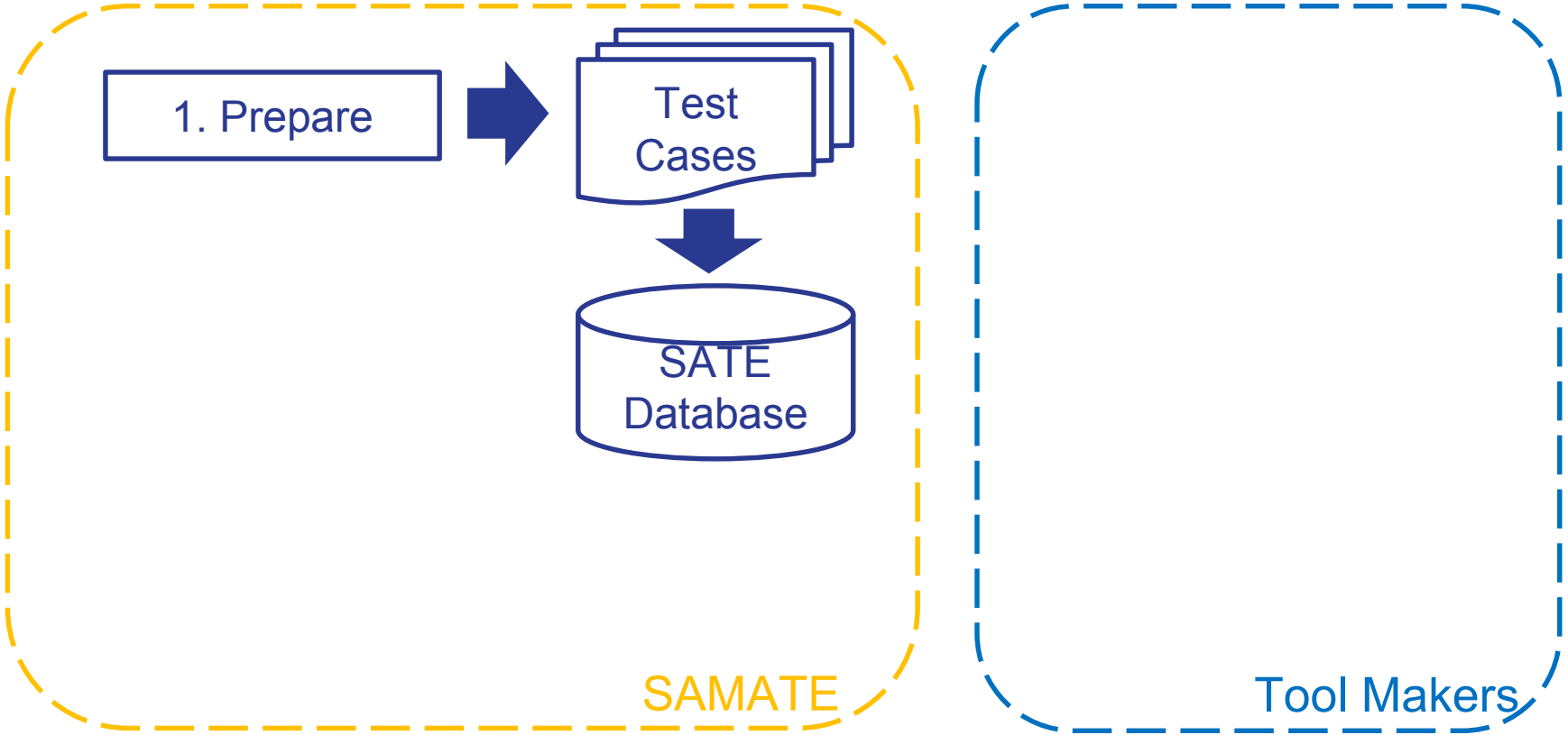
- Our analysis procedure has limitations
- In practice, users write special rules, suppress false positives, and write code in certain ways to minimize tool warnings
- There are many other factors that we did not consider: user interface, integration, etc.

- So do NOT use our analysis to rate/choose tools,
  but we encourage you to use our test cases and methodology

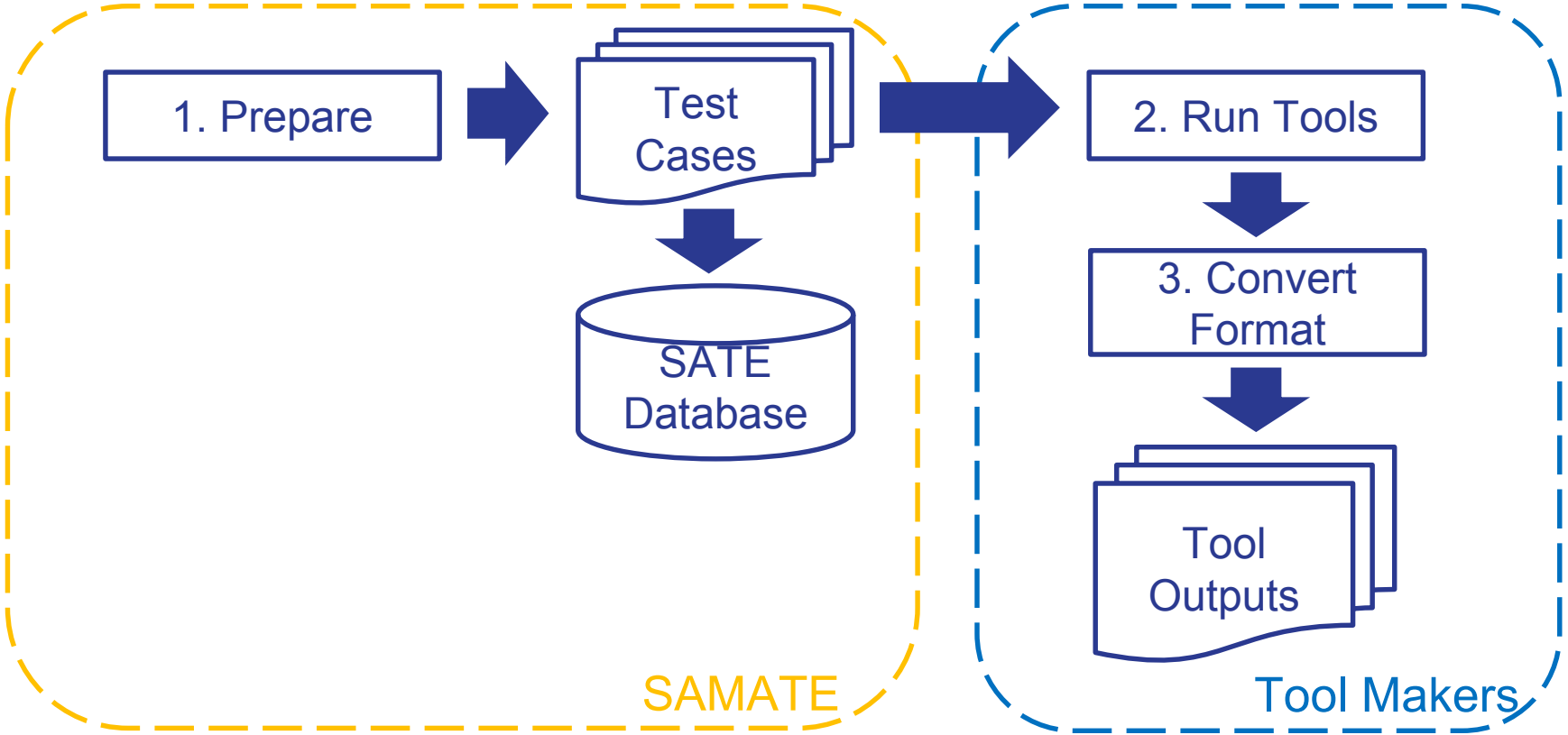
SATE Goals

- Enable empirical research on large test data
- Feedback for tool makers
- Increase public awareness
- Collaborative environment
- Focused on security-relevant weaknesses

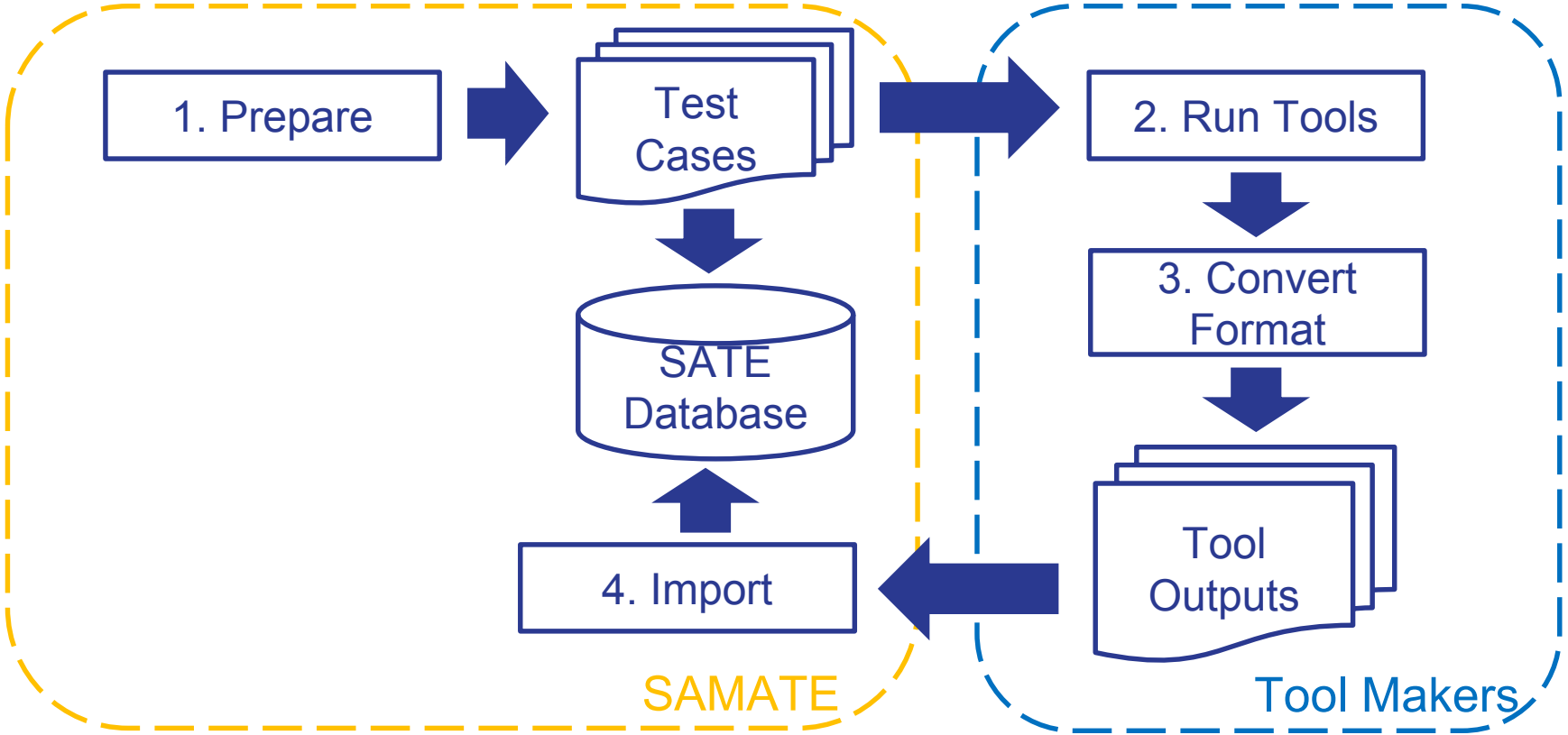
Procedure



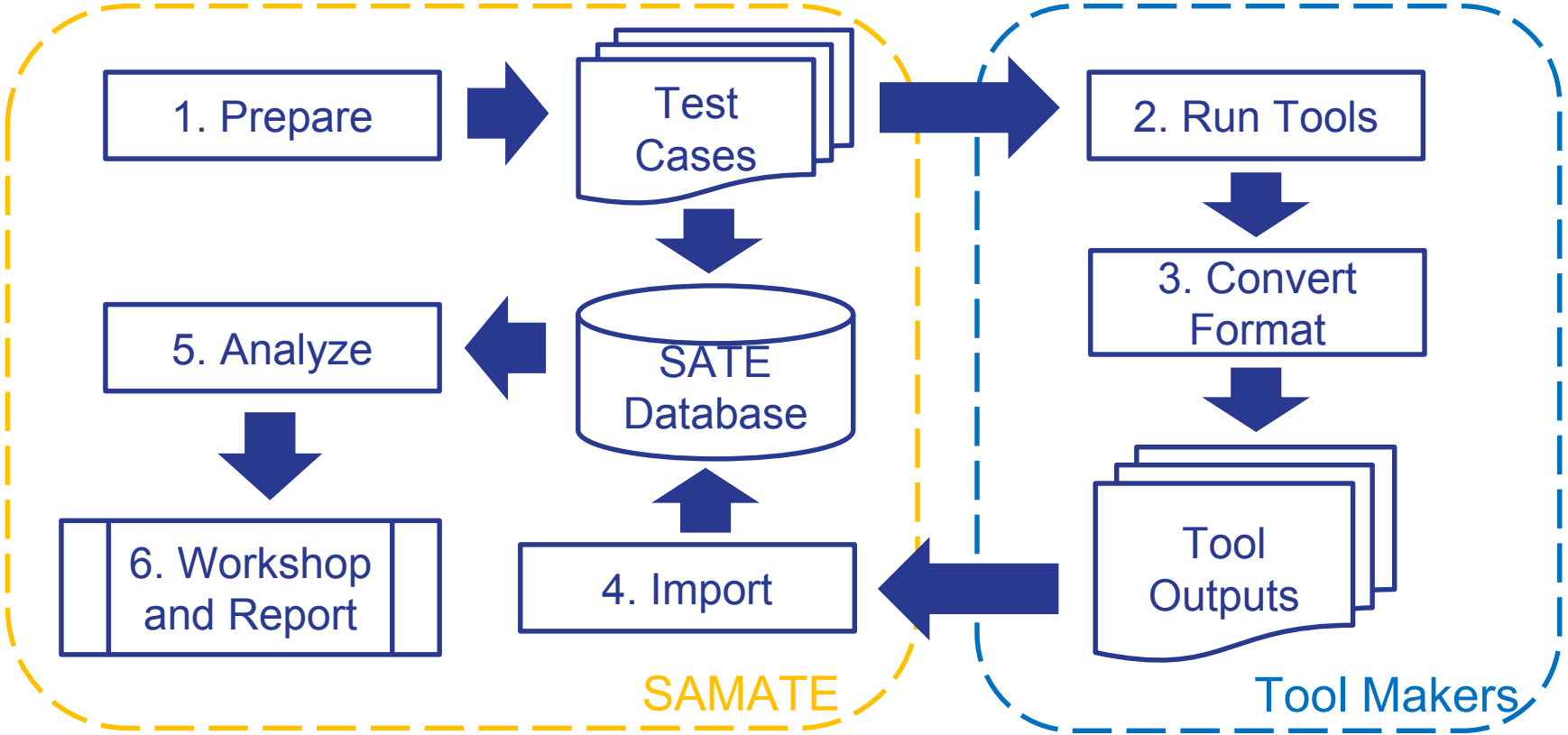
Procedure


1. Prepare
Test Cases
SATE Database
SAMATE
2. Run Tools
3. Convert Format
Tool Outputs
Tool Makers

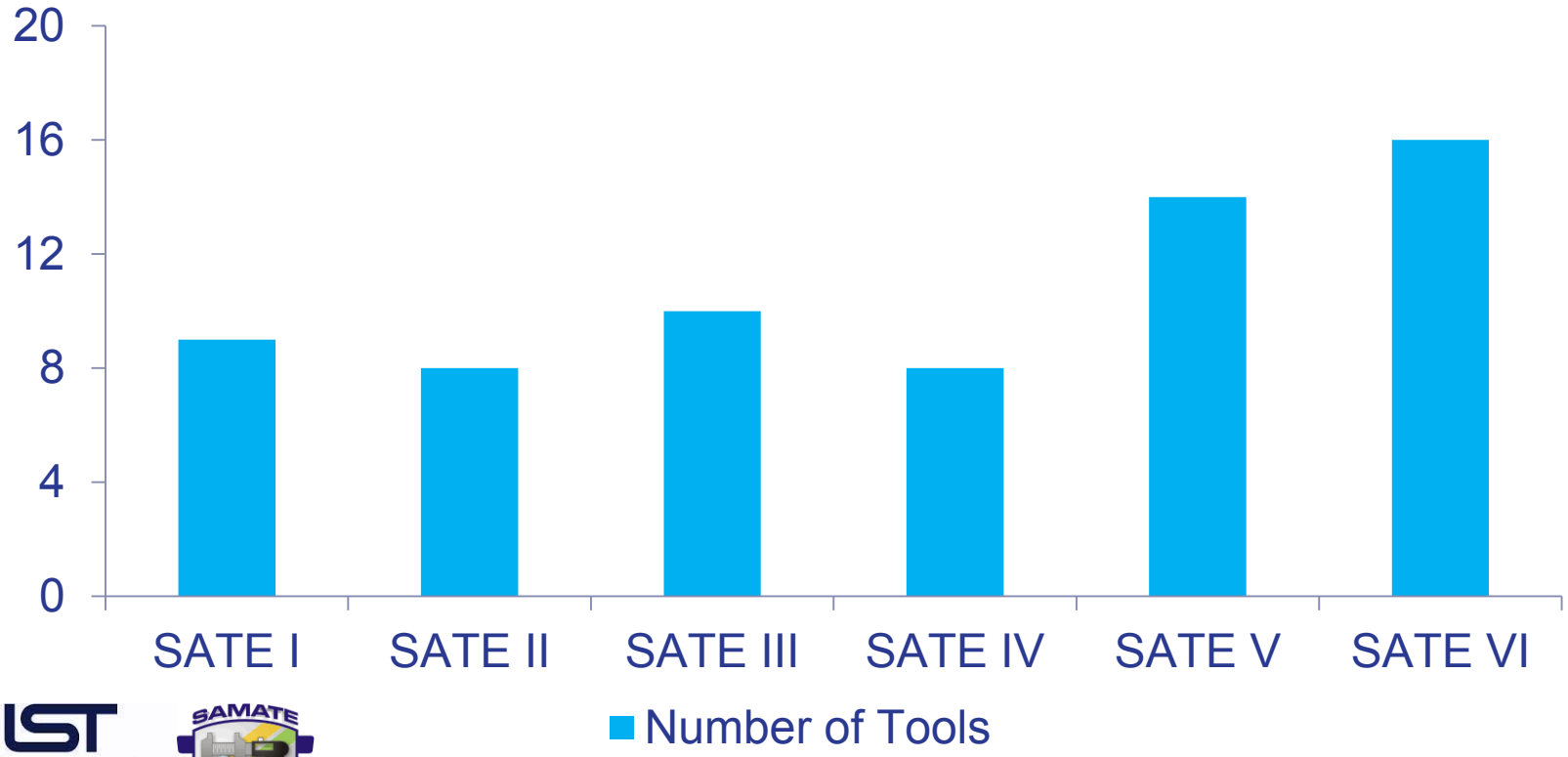
Procedure


1. Prepare
Test Cases
2. Run Tools
3. Convert Format
SATE Database
Tool Outputs
4. Import
SAMATE
Tool Makers

Procedure


1. Prepare
Test Cases
2. Run Tools
3. Convert Format
Tool Outputs
4. Import
SATE Database
5. Analyze
6. Workshop and Report
SAMATE
Tool Makers

Participation



NIST National Institute of Standards and Technology U.S. Department of Commerce

SAMATE

SATE VI Tracks

- Classic – (C and Java)
  - Focus on bug injection and collection
- Ockham – sound analysis tools (C/C++)
  - Limited size and coverage, but all findings are correct
- Mobile – tools for Android apps (not restricted to static analysis)

Participants

- Astrée
- Checkmarx
- Clang
- Cppcheck
- Flawfinder
- Frama-C
- Grammatech
- Gimpel
- Infer
- Kiuwan
- Mathworks
- Microfocus
- Parasoft
- Spotbugs
- Synopsys
- Viva64

Certain instruments, software, materials, and organizations are identified to specify the exposition adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the instruments, software, or materials are necessarily the best available for the purpose.

Classic Track

- Manually Collected and Injected Bugs
- Buggy and fixed versions

- Wireshark – network protocol analyzer
- DSpace – content management system
- Sakai – learning management system

NIST National Institute of Standards and Technology U.S. Department of Commerce

SAMATE

Automatic bug injection

- SQLite – relational DBMS
  - Buffer errors
  - Used GrammaTech bug injector tool
  - Based on the Software Evolution Library

Certain instruments, software, materials, and organizations are identified to specify the exposition adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the instruments, software, or materials are necessarily the best available for the purpose.

Cyber Grand Challenge / Trail of Bits cases

- Released by Defense Advanced Research Projects Agency (DARPA)
- About 200 challenge sets
- Small, simple versions of interactive services, like news or messaging
- Analysis still in progress

Facilitation

- Test cases released using Docker

- SATE output format
  Or
- OASIS Static Analysis Results Interchange Format (SARIF)