MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY

Technical Excellence...Tactical Value

Marine Corps Tactical Systems Support Activity

Informational Briefing

Optimizing T&E with STAT, VM, and Automation

February 2019
UNCLASSIFIED

Purpose: To provide an overview of MCTSSA's use of STAT, VM, and Automation in DT&E

MCTSSA Mission

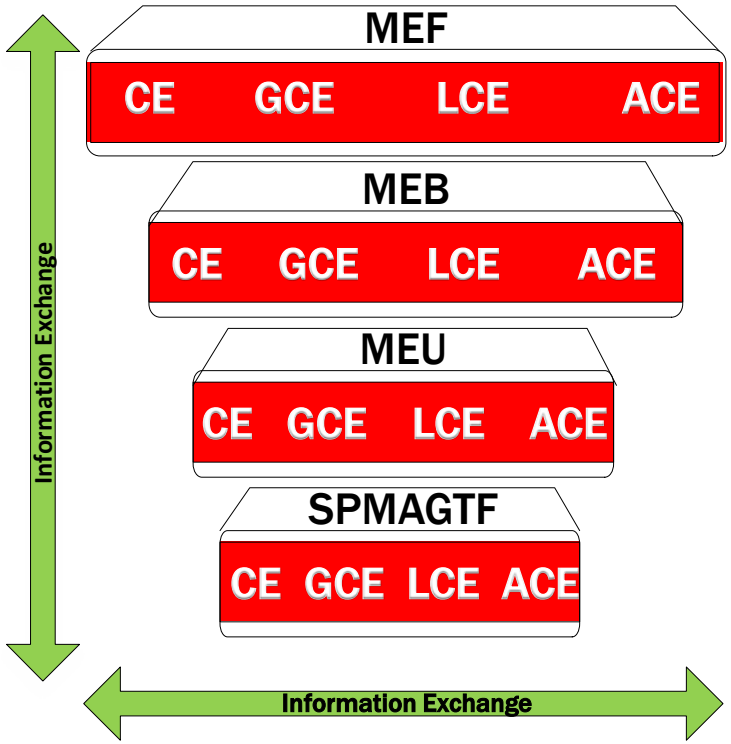
MCTSSA provides test and evaluation, engineering, and operating forces technical support for USMC and Joint Service command, control, computer, communications, and intelligence (C4I) systems throughout all acquisition life-cycle phases.

The Marine Corps' C4I Duty Experts

Test & Evaluation (T&E)

- Providing test expertise in developing:
  - Test Strategies and Plans
  - Test Procedures and Use Cases
- Conducting developmental, integrated, and joint certification test and evaluation
- Using operationally relevant C4I architectures
- Applying scientific test and analysis techniques

Vertical and Horizontal Test Threads



Disciplined Test and Evaluation Processes

Overview of How MCTSSA Tests

- Upon receipt of a system under test at MCTSSA, we create a virtual image of the SUT for use in the VSIE.

- We assess the virtual image's performance among MCTSSA's VSIE Server infrastructure in order to determine the risk of using the VSIE for developmental testing.

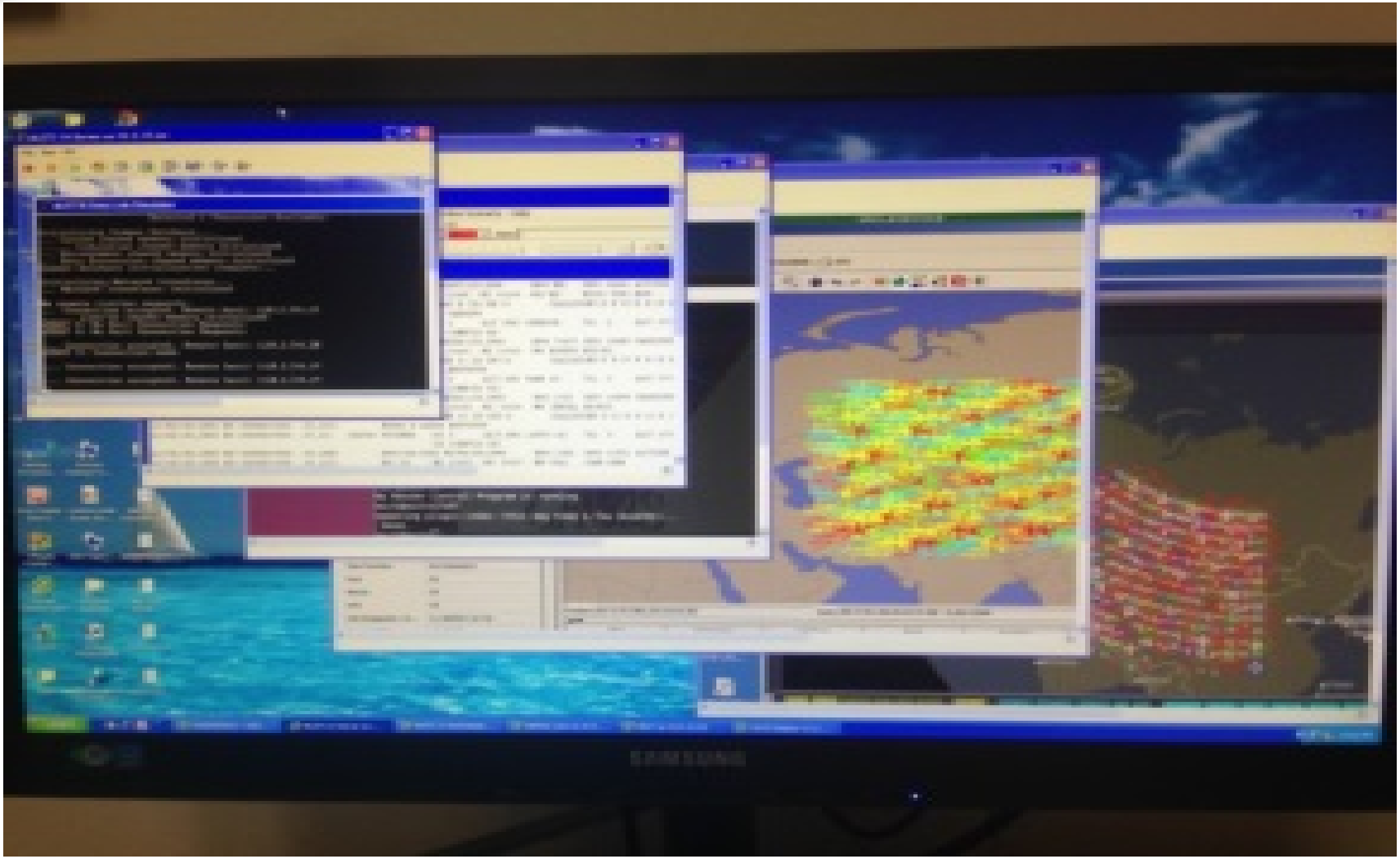
Overview of How MCTSSA Tests (cont)

- We compare the virtual image to the physical system under test (if available) in order to assess the risk of using the virtual image for developmental testing.

- If the risk of using the virtual image to the testing effort is minimal, then make the image available to all testers utilizing remote desktops and the virtual desktop infrastructure.

MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY

Technical Excellence...Tactical Value



Overview of How MCTSSA Tests (cont)

- Test Engineers participate in the Test and Evaluation Working IPT (T&E WIPT) in order to evaluate the test requirements and create a Data Capture and Analysis Plan (DCAP).

- The Test Engineers will create and support a strategy for utilizing test automation where applicable.

Test Case Matrix

Title	Description	Req #	Test Objective #	Test Case #	Estimated Duration
Title	Description			1	
Title	Description			2	
Title	Description			3	
Title	Description			4	

Data Capture Requirements

Test Case #	Metric Description	Data Element	Units of Measure	Expected Range	Method	Data Collection Tool(s)
1						
2						
3						
4						

Test Tools

Tool Name	Tool Description	Data Element(s) Captured
Data Collection Tools		
Simulation/Stimulation Tools		
General Test Tools		

Test Results Summary

Test Case #	Test Case Name and Description	Objective	Met Partially Met or Not Met?	TIR #
1				
2				
3				
4				

Overview of How MCTSSA Tests (cont)

- Test Engineers and T&E WIPT members will utilize the Virtual Systems Integration Environment (VSIE) to create, dry-run, and evaluate the test procedures as well as evaluate the DCAP.

- If TIR's are created against the virtual system under test, then determine if the TIR can be replicated with the physical system.

Manual vs Automated testing

- Manual testing is performed by a person sitting in front of a computer carefully executing the test cases
- Automation at MCTSSA is using a tool to execute test cases
  - The automation SW can also enter test data into the system under test, compare expected and actual results and generate detailed test reports

Tools Identification

- Identify the requirements
  - Automated Test Tools for MCTSSA testing
- Explore various tools and capabilities
  - SAGE, Robot, Selenium, Winium, Sikuli and ATRT (currently)
- Set the expectation from the tool(s)
  - Limitations and Capabilities of these tools

Automation Examples

- ATRT
  - Replicate operation acting upon a GUI
    - Email
    - Sharepoint
    - VMF (Mil-Std 2017) messages
- SolarWinds
  - Collect application layer network traffic
  - Collect datalink and network layer communications
- Ixia Breaking Point
  - Transmit realistic network traffic
- Sn1per/Sparta/Nmap
  - Scan network/discover hosts
  - Launch automated “cyber regression” tests

USMC C4I system automation: CAC2S

- ATRT Test Manager (to test SUT message transmission processing)
  - MILSTD- 6016 messages transmitted via GUI
  - Combinatorial Test generated test cases
- MLST3 (to test SUT message reception processing)
  - Scripted scenario for transmitting same messages
  - Data reduction tool for binary to ASCII conversion
- MANDRIL and ATRT Analysis Manager
  - Perform binary analysis of MILSTS 6016 message traffic

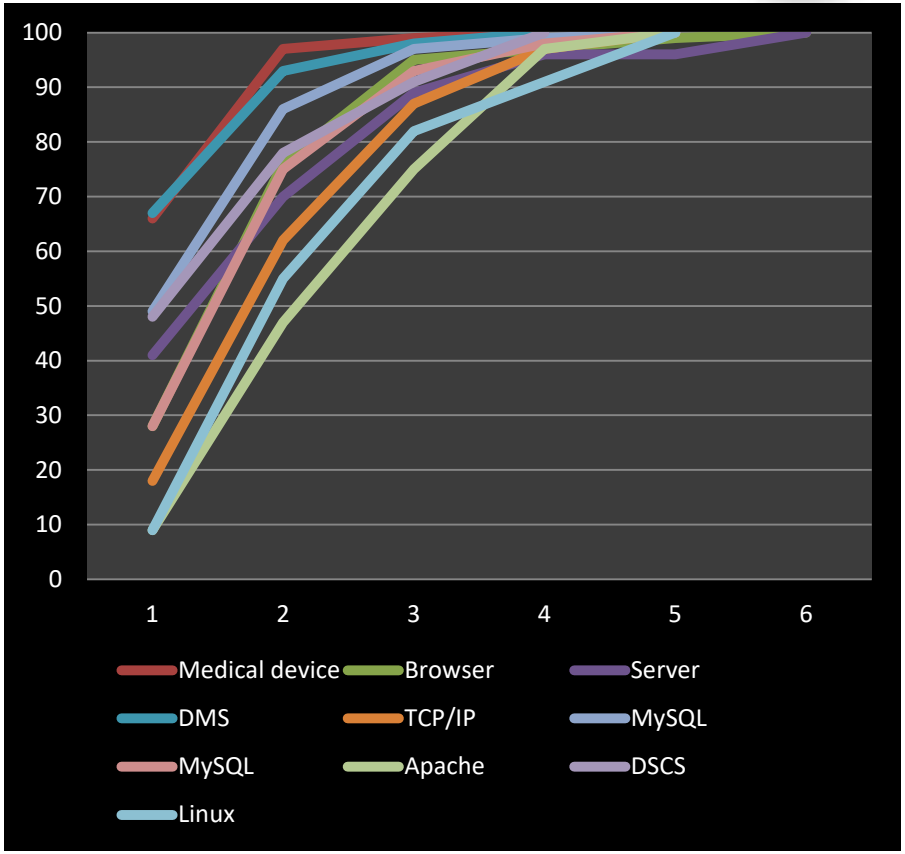
Automation inputs

- Combinatorial Testing used to produce test cases
-

TC	LAT	LONG	ALT	ID	EX	EMG	SIM	BEA	SPE	AMP	AMP CON	BOOST	PLATFORM	ACTIVITY	SPECI
1	33:00:00 N	117:00:00	NULL	0	0	0	1	0	250	DEBRIS	0	0	SATELLITE	RECONNA	ASHU
2	33:15:00 N	117:00:00	100000	1	1	1	0	30	350	WARHEAD	1	1	WEAPON	ANTISPAC	TAEP(
3	33:30:00 N	117:00:00	50000	2	0	0	1	45	450	HIGH EXPL	2	0	BASE (SPA	SURVEILLA	SS-N-
4	33:45:00 N	117:00:00	25000	3	1	1	0	60	550	BOOSTER	3	1	METEOR	DATA LINI	DELTA
5	34:00:00 N	117:00:00	10000	4	0	0	1	75	650	ACM	4	0	SPACE GEI	ELECTRON	HATF
6	34:15:00 N	117:00:00	NULL	5	1	1	0	90	750	DECOY BA	5	1	BALLISTIC	COMMUN	JERIC
7	34:30:00 N	117:00:00	11111	6	0	0	1	115	200	CHAFF	6	0	DEBRIS (O	RETURN T	AL-FA

Empirical studies have shown that three-way interactions, or combinations, can effectively find an average of 90 percent of the software faults and with fewer test cases than exhaustive manual testing.

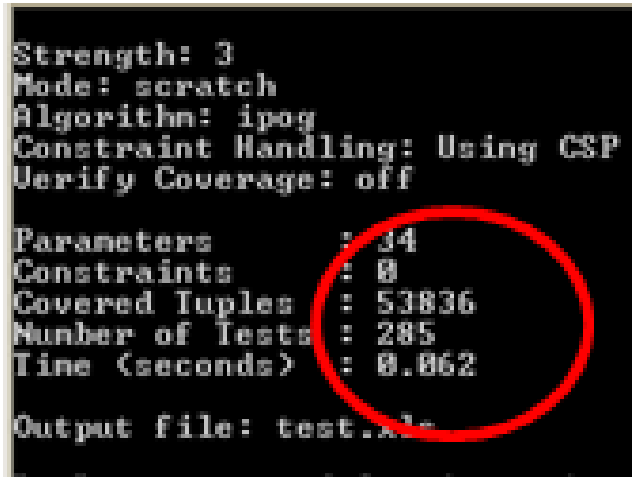
"Interaction Rule: Most failures are induced by single factor faults or by the joint combinatorial effect (interaction) of two factors, with progressively fewer failures induced by interactions between three or more factors."

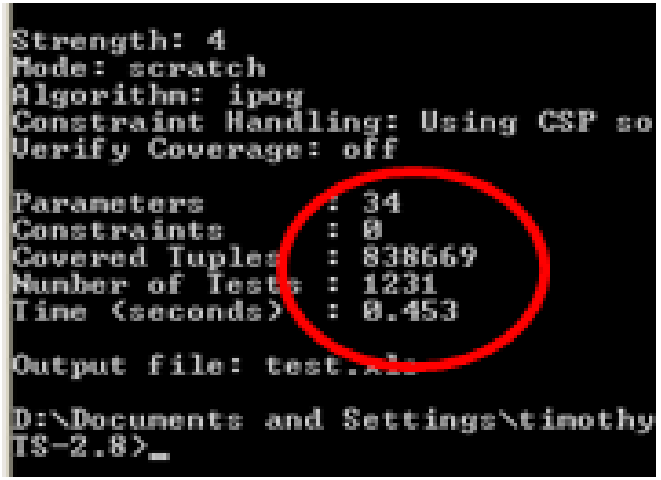


https://csrc.nist.gov/projects/automated-combinatorial-testing-for-software

Let's Apply CT to a J3.2

- For the J3.2, there are 371,589,120 valid test combinations of the 34 message fields
- Using combinatorial methods, that large number of test cases can be reduced to 285 test cases if testing all three-way combinations.

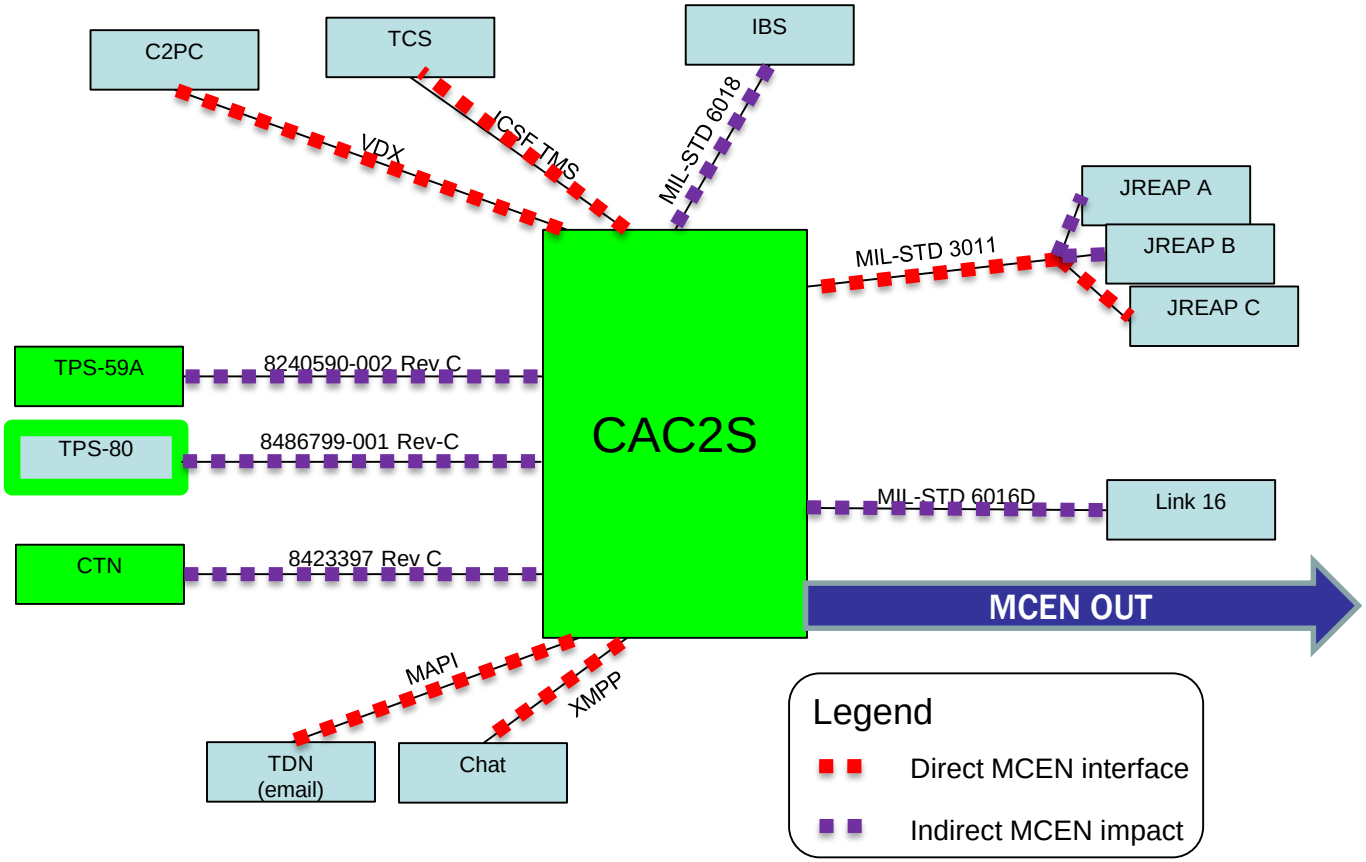




DOE Approach for MCEN Planning Yard (MPY)

- A Design of Experiments (DOE) approach was used to characterize the factor contributions to network performance.
- The design was a two-level fractional factorial that quantified the main effects and interactions of the eight factors being considered.
- Using statistical analysis techniques, we assessed which effects were statistically significant as compared to system noise using the response of "bits per second" as the primary measure of performance.

MCEN Interfaces



Persistent Virtual (VM) Configurations

New System Under Test (SUT)

Tactical Message Interoperability
Joint and Service Level Collaboration in a Persistent Environment

Automation
Constantly running test cases

STAT
Scientific Test and Analysis Techniques

Virtualization
Always On Physical & Virtual Infrastructure

Link 16

Tactical System 1

VMF

Tactical System 2

Benefits

- Insights & Actions
- Automation & Analytics
- Security & Compliance

CYBERSTAT

- CYBERSTAT is applying Scientific Test and Analysis Techniques (STAT) to offensive cyber penetration testing tools

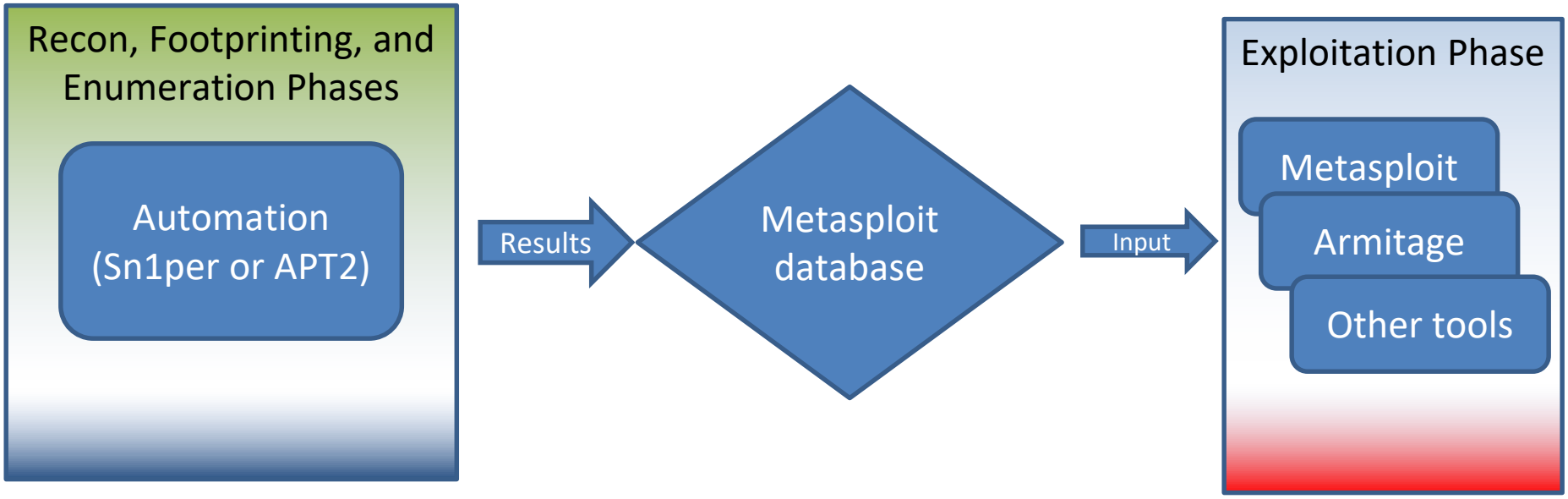
- Not this...

CyberStat
https://www.cyberstat.com/
Home Climate Control From Anywhere.

- By applying STAT to the tool, the tool's scope is expanded beyond "one at a time" uses as combinations of options are explored with a Combinatorial Test

The penetration test tool is the system under test
A test case passes if the tool finds a unique vulnerability

Cyber, STAT, and Automation



CYBERSTAT Is Utilized For Test Case Input Once Automation Is Mature

How can Industry Help?

- Development and support of STAT design and analysis via tools and statistical expertise
- Provide automation support/expertise for current and future C4I systems testing
- Provide knowledge and tools to maximize utilization of virtualization technologies in support of C4I testing
- Provide a way to measure/quantify how much Cyber testing is required vs how much is actually performed.

MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY

Technical Excellence...Tactical Value

Questions?