Army Test & Evaluation Office
Cyber Shift Left

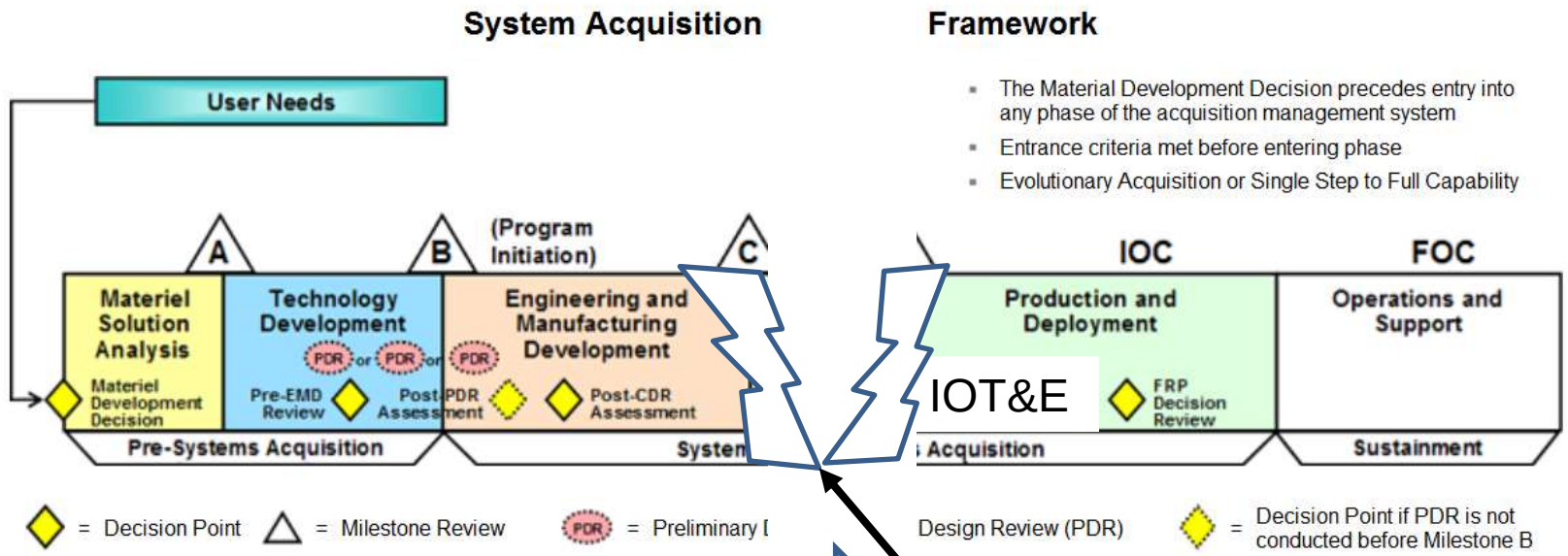
Mr. David Jimenez

to

ITEA

16 March 2016

Cyber Security Current Situation



- The Material Development Decision precedes entry into any phase of the acquisition management system
- Entrance criteria met before entering phase
- Evolutionary Acquisition or Single Step to Full Capability

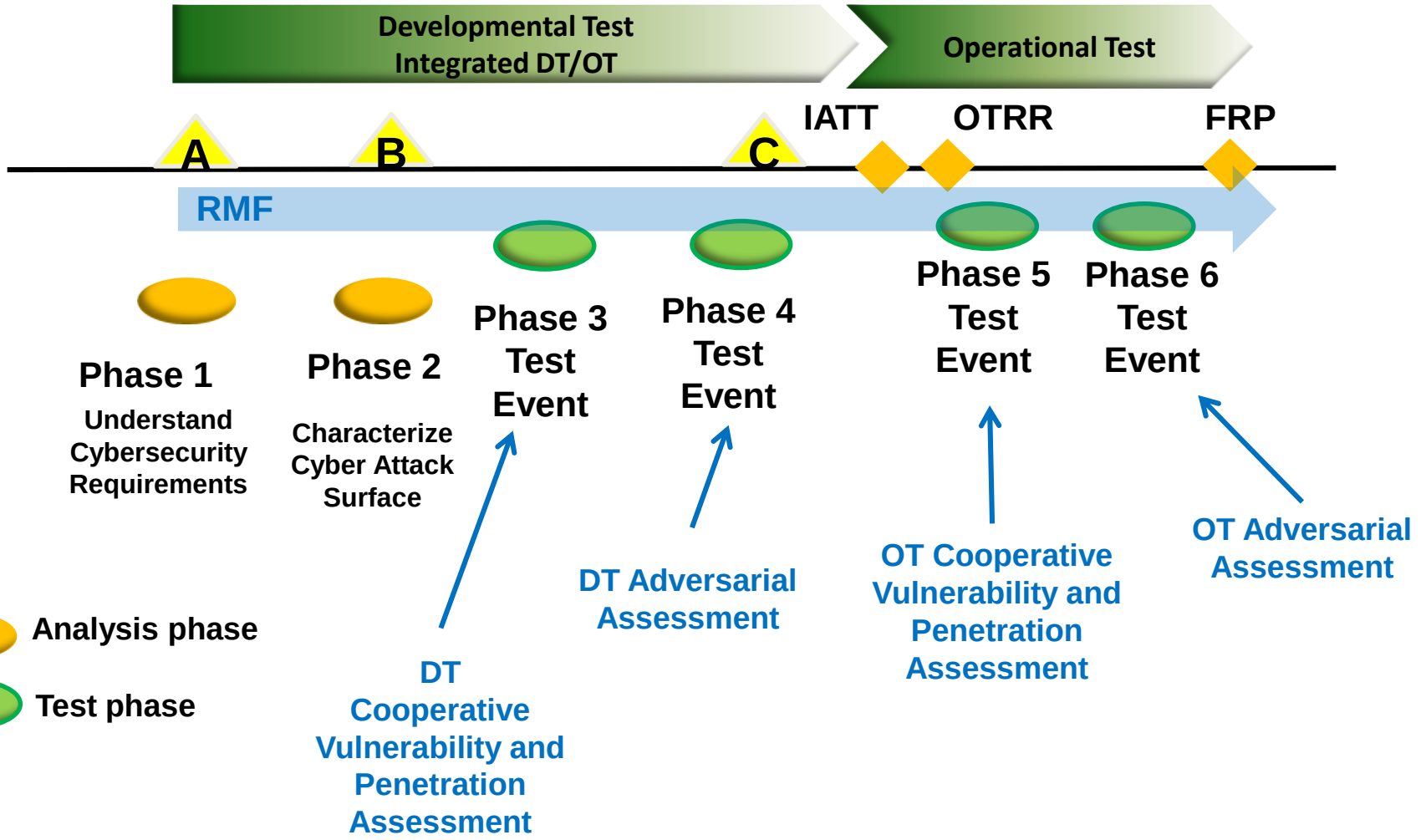
Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

- **"Pre-Milestone A to Retirement"**
  - ❑ **Duration of a System Lifecycle - Continuous Process**
  - ❑ **Establish Security Architecture Early**
  - ❑ **T&E of Major Software Drop in DT and OT**
  - ❑ **Software Changes in Sustainment**

"Must close this gap to enable unity of effort"

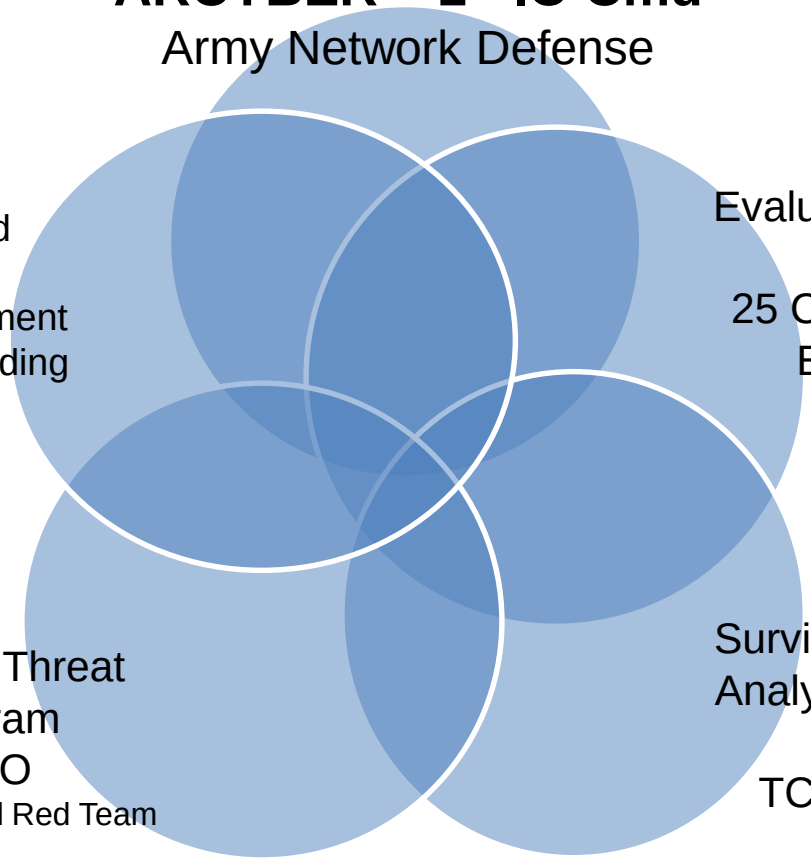
Shift Left

Cybersecurity T&E Earlier Than IOT&E



Events derived from draft DASD(DT&E) DoD Cybersecurity Test and Evaluation Guidebook, and DOT&E Cybersecurity Operational Test and Evaluation Guidance Memo (01 August 2014)

Multi-Discipline T&E Cyber Teams



ARCYBER – 1st IO Cmd
Army Network Defense

TRADOC
Development, coordination, and approval of the operational environment (OE) portrayal, including threat forces (DOTMLPF)

ATEC
Evaluation of Army Material
25 Cybersecurity Evaluators

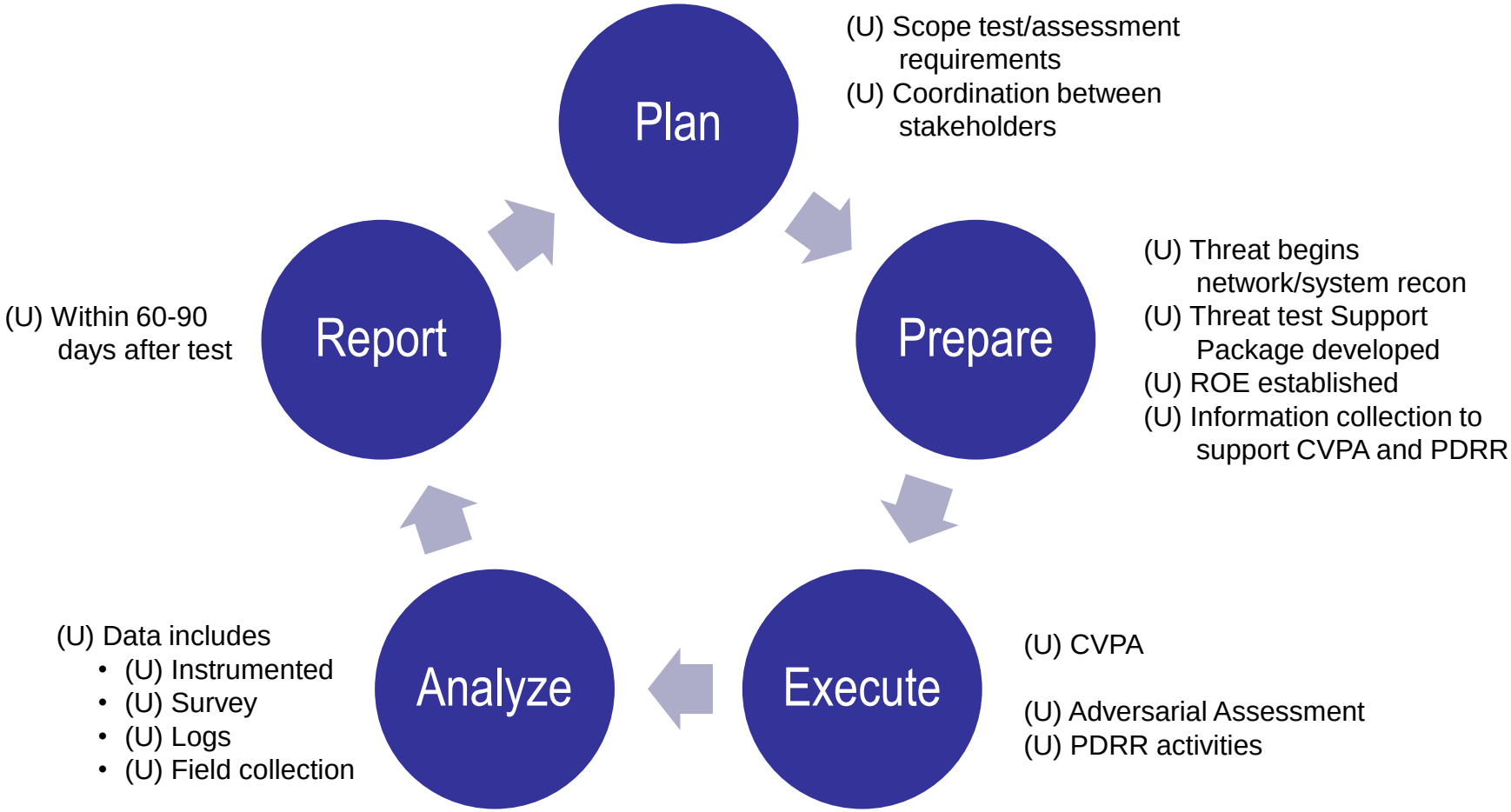
TSMO
Manage the Army Threat Systems Program
40 CEH/TCNO
USSTRATCOM Accredited Red Team

ARL/SLAD
Survivability and Lethality Analysis of Army Material
36 CEH
TCNO/Cybersecurity

Acronyms
CEH – Certified Ethical Hacker
TCNO – Threat Computer Network Operations
DOTMLPF – Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities

<100 qualified personnel for T&E
Of Cybersecurity

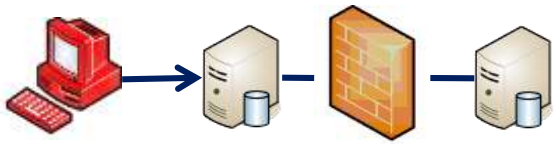
General Cybersecurity T&E Event Calendar



(U) For CCMD and Operational Tests, this cycle is a one-year process

Generic Anatomy of a Hack

1. Through reconnaissance, attacker identifies an accessible web server. Enumerate web server, identify exploitable vulnerability



2. Exploit server, look for account credentials and path to internal network

3. Using valid account, stolen in step 2, access server on internal network

4. Seek additional account credentials, identify workstations and domain controllers

5. Using valid (stolen) credentials, access user workstations. Set up persistent foothold. Look for administrator accounts to harvest.

6. Locate local administrator token, once found dump domain SAM (password) file. Begin cracking SAM offline.

7. Attacker now likely to have access to many accounts. High probability one is domain administrator (has keys to kingdom)

8. Access to internal network established. Transition to data mining and/or seek mission critical systems and position to deny/degrade/disrupt mission.

Threat Capabilities:

- Novice
- Intermediate
- Expert

Threat General Characterization

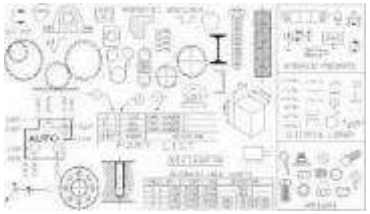
- Insider: Legitimate PHYSICAL and/or LOGICAL access
- Nearsider: Physical access with NO legitimate LOGICAL access
- Outsider: NO legitimate PHYSICAL or LOGICAL target access

Test Rigor: NIE Cyber Time Line

Date	Outsider Threat	Nearsider Threat	Insider Threat	Overall Objectives	Desired results/actions
Ongoing	Continues During Test			OSINT research	Develop intelligence on SUT
09 Jan 2015				Receipt of Published LDIF (TCNO IP addressing)	Ensure quantity and location of Threat IP support the Threat IP requirements
09 Mar – 03 Apr	VALEX			Complete CVPA for all SUTs (Blue Team)	Discover vulnerabilities and mitigate as possible for SUTs and have 1st IO BVAT look at integrated network.
22 – 23 Apr 2 days (All Sites)	Field COMMEX			Conduct Threat IP test, Check LDIF for Threat IPs	IP address space that is allocated for and usable by TCNO team.
22 – 26 Apr 5 days	Process and Product (OPFOR COP with CNO) in IW TOC			Data collection and passive scans and reconnaissance	Scan data to be used by threat CNO team to ascertain network posture.
27 Apr - 01 May (All sites)				Data collection and passive scans and reconnaissance Participate in EW Verification Practical Exercise as appropriate	Collaborative threat environment
Date	**Outsider Threat**	**Nearsider Threat**	**Insider Threat**	**Overall Objectives**	**Desired results/actions**
27 Apr – 01 May Pilot Test (All Sites)	Network Discovery and Target Development			Data collection and passive scans and reconnaissance	Scan data to be used by threat CNO team to ascertain network posture. Posture TCNO to attack the network.
05 – 17 May Record Test (All Sites)	Active Network & Signal Discovery. Reconnaissance of network characteristics; prepare to eavesdrop.	Passive & Active Network Scanning; network reconnaissance.	System Probing; Directory traversal; Machine Learning.	Learn network topology; Ascertain each target's value; Find susceptibilities in network & computer devices. Conduct CNE and CNA	Posture the threat CNO team to be able to attack the network.

AEC Strategy Toward Improving Cyber Security Performance of Systems Under Test

The Risk Metrics are designed to drive the improvement of operational security in enterprise networks via an OODA Loop



Design	Development	Developmental Testing	Operational Testing	Operational Environment

Shift Cyber Security Concerns Left