Marine Corps Operational Test and Evaluation Activity

Cyber Division Brief to ITEA Conference

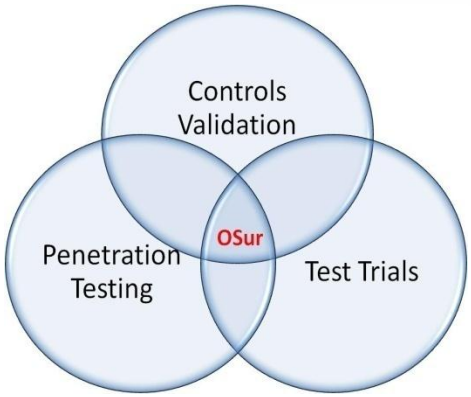
26 February 2015

Our job in Cyber Security is to ensure the technological advantage our fighting men and women have in the face of adversity, remains intact. We protect the hard-won intellectual property that protects those that place themselves in harm's way. It is our responsibility to defend the edge developed for our warfighters from those that would take it. We are the Cyber Guards protecting the information that furnishes a degree of security to our forces. We are here because they are there.

Q1

- **How are the OTAs/Services/DHS currently evaluating DT and OT data/events currently?**
- **How do you see that changing, or what is the evaluation framework for the future?**

Answering OSur (CS Process)



OT&E

Test trials that exercise the User and Administrator while in an Operational environment.

CIA: Confidentiality, Integrity, Availability

Penetration Testing

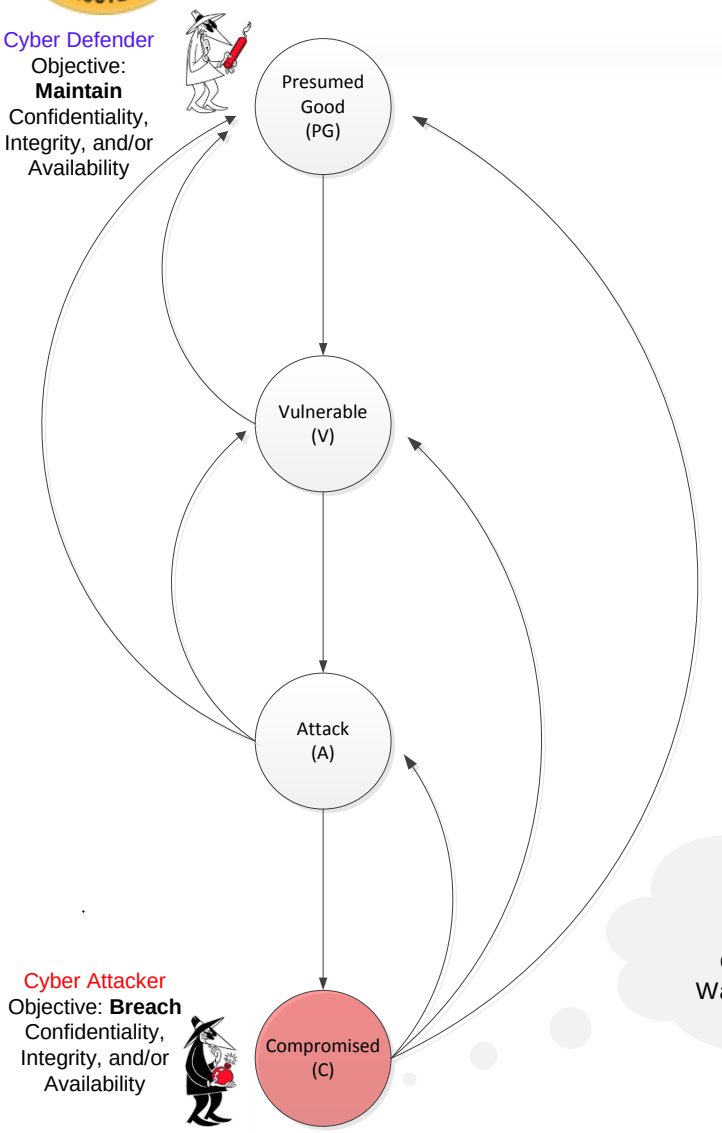
Provides a more in-depth view of a systems IA posture by determining if each control as implemented by the program office answers PDRR (Protect, Detect React, Restore) .

Controls Validation

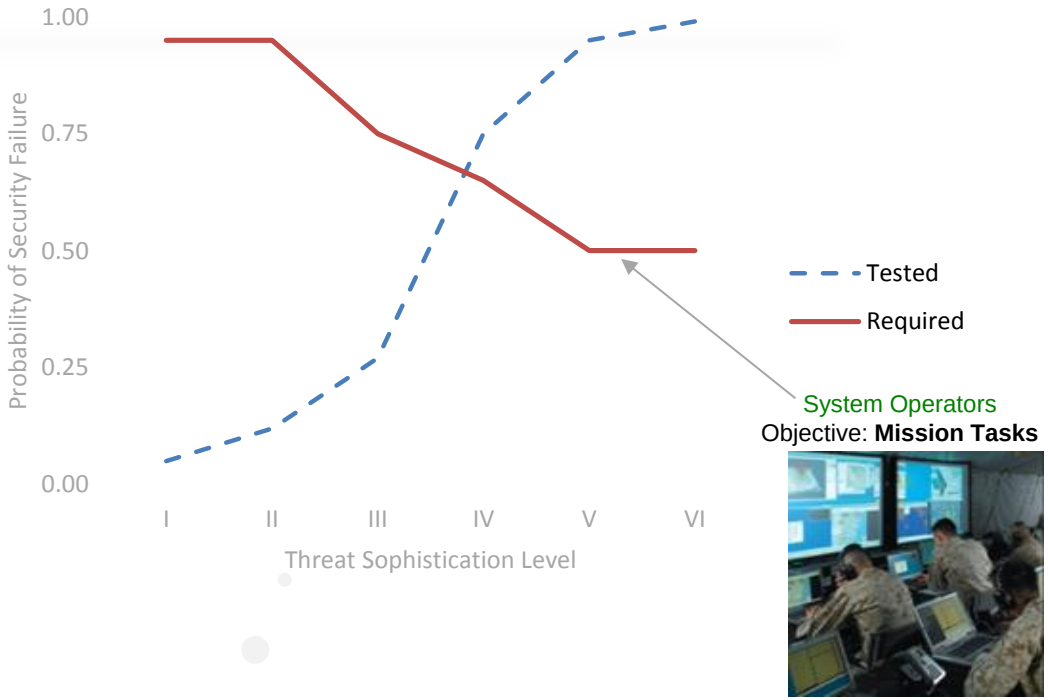
Provides a detailed view through a Technical and Non Technical Assessment of each control that as implemented by the program office answers PDRR (Protect, Detect React, Restore) .

Executing MCOTEAs building block approach supports the system engineering process while managing an acceptable level of risk at each milestone.

The Future of Cyber in OT and Assessment



Novice, Cyber-punks, Petty Thieves, Virus Writers, Professional Criminals, Information Warriors, Political Activists

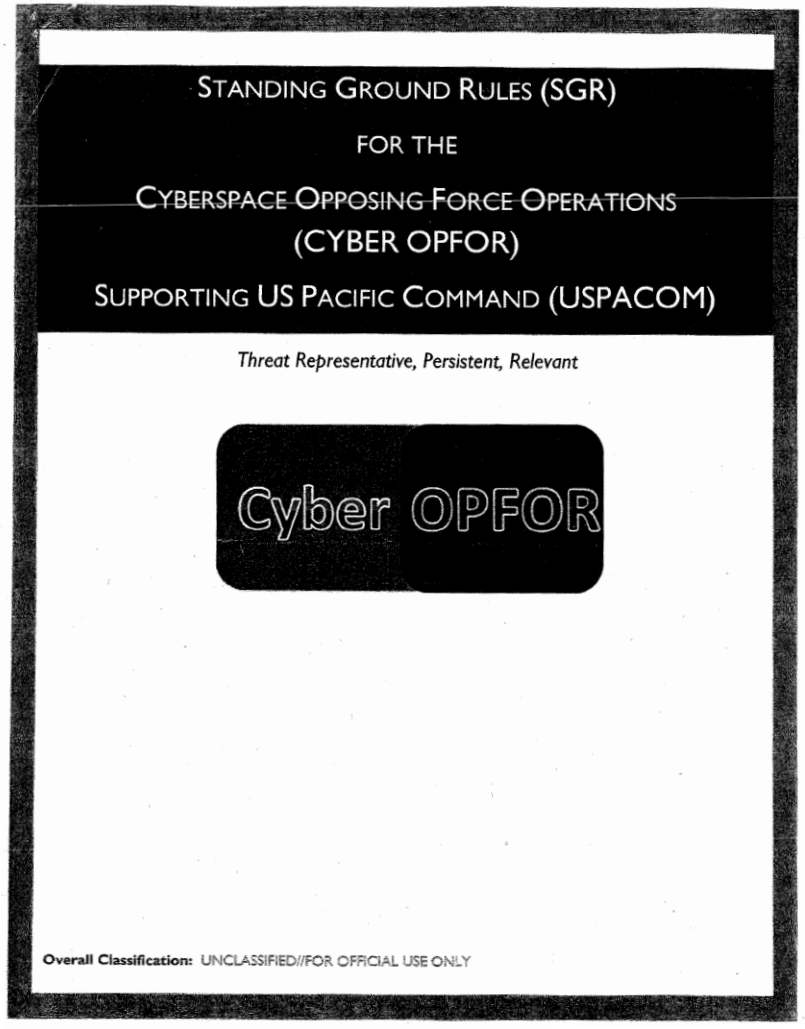


Operational Testing will quantitatively answer this basic question:

"*What level of availability, confidentiality, and integrity does the [network/ network system] provide of network/data in a realistic threat environment?*"

LEVERAGE

Persistent Threat or Continuous OpFor



STANDING GROUND RULES (SGR)

FOR THE

CYBERSPACE OPPOSING FORCE OPERATIONS

(CYBER OPFOR)

SUPPORTING US PACIFIC COMMAND (USPACOM)

Threat Representative, Persistent, Relevant

Cyber OPFOR

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Signatures:

  Thomas L. Conant
  Lieutenant General, U.S. Marine Corps
  Deputy Commander, Pacific Command
  (Requesting Command)

  Kerry E. Kelley (16 Jan 14)
  SES,DAF
  Director, C4 Systems, USSTRATCOM

  Brett T. Williams (08 Jan 14)
  Major General, United States Air Force
  Director of Operations, USCYBERCOM

  DOT&E (18 Feb 14)
  J. Michael Gilmore
  Director, Operational Test and Evaluation

Q2

- **What are typical evaluation metrics and do they vary between DT and OT-type events?**

Evaluation Metrics

- Using the Net-Ready KPP Language out of the CJCSI 6212.01E/F as the primary basis for our Measures (Wrapped with the Persistent Threat)
  - 5 Elements (E)
  - 3 Attributes (F)

- Fully integrated teams to ensure consistency across ACAT (IVT) to ACAT I Marine Corps programs
  - **Lacking this on Joint programs**

Pending Cyber KPP (DepSecDef)

DoN, J6, J8 and DOT&E

Q3

- **What automated tools or M&S are being used to support evaluations?**

Cybersecurity Tools

Green Team

- Solar Winds Toolset
- Vulnerator
- SCAP Compliance Checker
- BlueScope
- Lan Sweeper
- SkyBox
- Retina/ACAS
- Nexpose
- NMAP
- USB Detect

Blue Team

- Qtip
- Nexpose
- NMAP
- Retina/ACAS
- Wireshark
- Vulnerator
- SCAP Compliance Checker
- Lan Sweeper
- Solar Winds Toolset
- USB Detect
- SkyBox

Cooperative Pen Test

- Hash Cat
- Cain & Abel
- Burp Suite
- Web Scarab
- NMAP
- Wireshark
- Armitage
- Flying Squirrel
- Nexpose
- Metasploit
- Lophtcrack
- Kali Linux
- Retina/ACAS
- John the Ripper

Q4

- **How are the Services/DHS accounting non-hardware aspects of cyber security—operator training, CONOPS—in evaluations?**

Non Technical Evaluation

- Through the use of:
  - Questionnaires
  - Observations
  - Document reviews (ATO, CONOPS, CP, IAVA Management Plan, 3rd Party Patching Plan, CM Plan etc..)
  - Cyber Security Evaluation Tool (CSET) which is a self-assessment tool

This evaluation is just as important as the technical evaluation to ensure we capture a complete view of the program

Q5

- **What collaboration is occurring between the OTAs/DHS and other Federal Agencies to develop best practices and leverage tools and methodologies?**

Division Interaction

Internal to the Marine Corps

- MCCDC (Cyber)
- MARFORCYBER
- MSTP
- MAGTFTC
- PP&O (Cyber Advocate)
- I, II, III MEF (G2, G3, G5, G6, CoS and MSC's)
- Base G-6's
- HQMC C4 (Cyber and CIO)
- MCNOSC
- MCIA
- MARCORSYSCOM
- TECOM

OSD Cybersecurity Program

- ATEC
- AFOTEC
- COTF
- JITC
- DIA
- NSA