TUTORIAL DESCRIPTIONS

2020 Cybersecurity Workshop

Monday, November 16th 8:00am – 12:00pm

Cyber Table Top (CTT) Workshop For Participants & Facilitators

Instructor: Vincent Lamolinara, Defense Acquisition University

The tutorial introduces and applies the Cyber Table Top (CTT) mission-based cyber risk assessment (MBCRA) method to help discover cyber vulnerabilities, gauge their risk, propose mitigations and inform other competencies, documents and events across the DoD acquisition lifecycle. The workshop will establish an understanding of the threat and "thinking like a Hacker"; provide a "wheel of access" methodology to identify and diagram surface-attack characteristics; include cross-competency personnel, including users, to identify and prioritize cyber-attacks / vulnerabilities in a Red / Blue / White Team "wargame" mission scenario; and provide a construct to characterizes and report risk and mitigations in order to design and maintain cyber resilient systems and personnel in the acquisition and operational phases of an Information or Platform weapons system. Participants will conduct exercises in each phase to reinforce and apply the concepts and methodology will learn how cybersecurity principles apply to their career fields. Students will create a surface attack taxonomy, role play different competencies including engineering, test, cybersecurity, logistics, safety, intelligence, contracts and the adversary. The case studies and scenarios will build up in complexity culminating in a mini-CTT execution and Cyber Risk outbrief (to a simulated PM) for an exemplar weapons systems at the UNCLAS level. Students will also apply CTT results to inform Test, AoA ICD/CDD/CPD, RFP/SOW, Specification, Architecture and upgrade / patch / ECP requirements as well as acquisition and risk management strategy. This workshop will allow enable students to participate in CTT efforts in their respective programs. Tailorable to the specific customer needs. Objectives : Given a cybersecurity scenario, use Surface-attack characterization and Cyber Table Top Methodology to discover cyber vulnerabilities, gauge their risk, propose mitigations and inform other competencies, documents and events across the DoD acquisition lifecycle.

Learning Objectives

1. Understand and apply the "think like a Hacker" adversarial threat concept to cybersecurity.
2. Understand, apply and create the "wheel of access" surface-attack methodology to create a taxonomy useable to discover cyber vulnerabilities for DoD systems.
3. Understand and apply CTT methodology for various acquisition scenarios.
4. Create program manager level outbrief delineating risks, mitigations and implications for test, requirements, design, logistics and safety.

Target Attendees: The acquisition workforce, including industry partners, who design, build, procure, maintain, and provision cybersecurity capabilities.

Cyber Security Assessment of MIL-STD-1553
Instructor: Adam McCorkle, Georgia Tech Research Institute

The MIL-STD-1553 serial data bus standard has been around for over 4 decades and continues to be an integral network architecture on modern military aircraft, ground vehicles and both surface and subsurface ships. This presentation will provide a brief overview and history of the standard and then discuss potential vulnerabilities related to the physical, electrical, and functional characteristics that are inherent in implementations of the standard. In particular, modern cyber-attack techniques will be discussed that could potentially be applied to penetrate an implementation of the MIL-STD-1553 data bus. The severity of each of these intrusions will be examined and an overall risk assessment of these intrusion methods will be discussed. Lastly, ideas for potential attack countermeasures will be discussed that could potentially be applied to existing implementations of MIL-STD-1553 in order to mitigate these risks and to also drive engineering decisions for newly developed systems. This discussion in its entirety can aid with the development of a penetration testing program for a particular system or system of systems implementing the MIL-STD-1553 data bus.

Monday, November 16th 1:00pm – 5:00pm

Air Force's New MBCRA (Mission Based Cyber Risk Assessment) and Integrated Engineering Approach
Instructor: Kevin McGowan, 47CTS/OL-A (COLSA)

The AF commonly uses numerous stove-piped cyber vulnerability assessment processes, executed in parallel, to characterize cyber attack surfaces and to identify potential cyber vulnerabilities and risks. This is an inefficient use of limited resources and results in products being generated for targeted audiences (i.e., not usable by multiple stakeholders). It also results in less informed products and decisions.

The Mission-based Risk Assessment Process for Cyber (MRAP-C) is the AF's new iterative Mission Based Cyber Risk Assessment (MBCRA) process which builds upon best practices from the Cyber Table Top (CTT), Cyber Test Prioritization Methodology (CTPM), Cyber BlueBook (CBB), and integrated engineering processes. The MRAP-C combines bottom-up and top-down assessment approaches to identify critical components and system information, to assess potential cyber attack paths through the system, and to identify potential mission effects of cyber vulnerability exploitation. The MRAP-C analysis activities and Attack Path Vignettes generated during the MRAP-C process inform cooperative and adversarial DT and OT cyber test events, cyber test strategy, cyber test plans, cyber requirements, cyber test resource lists, and cyber recommendations development. It also fulfills Cyber Test and Evaluation Phase 1 and 2 requirements.

When combined with the USAF's integrated Program Protection / Systems Security Engineering (PP/SSE) Standard Process, programs are equipped with an iterative engineering process which assesses cyber vulnerabilities and risks throughout the acquisition lifecycle. When executed by the program's integrated Systems Security Working Group (SSWG), all member stakeholders are involved with performing the cyber vulnerability assessments and with performing key programmatic/engineering activities focused on developing a cyber secure and cyber survivable system for the warfighter.

This Tutorial provides an overview of the new USAF PP/SSE Standard Process, and the embedded MRAP-C MBCRA process, which is expected to become mandatory for all AF acquisition programs by the end of CY20.

Introduction to Cybersecurity Test and Evaluation
Instructors: Pete Christensen, American Systems and Jean Petty, The MITRE Corporation

The purpose of this tutorial is to familiarize attendees with Cybersecurity and Test and Evaluation as it applies to US Federal Government Programs and the U.S DOD. Note that the ideas and concepts presented also apply in principal to any acquisition program. Topics that will be addressed include Cyberspace as an operational domain, Cybersecurity threats, malware, DHS and DOD systems acquisition and associated Cyber T&E policy and process including "Cloud" Programs, requirements analysis, evaluation frameworks, cyber tabletop exercises, cooperative vulnerability assessments, adversarial assessments, cyber ranges and lessons learned.

TENA and JMETC Solutions for Cyber Test and Training
Instructor: Gene Hudgins, KBR

Together, TENA and JMETC enable interoperability among ranges, facilities, and simulations in a timely and cost-efficient manner. TENA provides for real-time system interoperability, as well as interfacing existing range assets, C4ISR systems, and simulations; fostering reuse of range assets and future software systems. JMETC is a distributed, LVC capability which uses a hybrid network architecture; the JMETC Secret Network (JSN), based on the SDREN, is used for secret testing and the JMETC Multiple Independent Levels of Security (MILS) Network (JMN) is the T&E enterprise network solution for all classifications and for cyber testing. JMETC provides readily available connectivity to the Services' distributed test and training capabilities and simulations, as well as industry resources. This tutorial will address the current impact of TENA and JMETC on distributed systems engineering as well as their significance to the cyber Test and Training community.