Join us for the 8th Cybersecurity Workshop

New Domains in Cybersecurity T&E

October 18-20, 2022
Embassy Suites by Hilton Destin Miramar Beach, Destin, FL
Hosted by the ITEA Emerald Coast Chapter

AGENDA

October 13, 2022

Registration Open Monday 3PM – 5PM Tuesday – Thursday 7AM – 5PM

Week at-a-Glance

EVENTS	DATE	TIME
Tutorials Separate fee and registration	Tuesday, October 18	8:00 a.m. to 12:00 p.m. 1:00 p.m. to 5:00 p.m.
Red Team/Blue Team Hands-on Lab Experience	Wednesday, October 19 Thursday, October 20	1:30 p.m. to 3:00 p.m. 1:30 p.m. to 3:00 p.m. 3:15 p.m. to 5:15 p.m.
Technical Track Sessions	Wednesday, October 19 Thursday, October 20	3:15 p.m. to 5:15 p.m. 1:30 p.m. to 3:00 p.m. 3:15 p.m. to 5:15 p.m.
Special Guest Speakers	Wednesday, October 19 Thursday, October 20	8:00 a.m. to 12:30 p.m. 8:00 a.m. to 12:30 p.m.
Networking Reception	Wednesday, October 19	5:30 p.m. to 7:30 p.m.

What is the ITEA Cyber Red/Blue Hands-on Lab Experience?

Understanding and implementing cybersecurity best practices are paramount to achieving data security, customer confidence, and positive financial growth for every organization across the spectrum. Organizations are challenged with defending their systems and information from malicious actors including nation states, insider threats, and non-malicious human error. Data destruction, stealing sensitive information, and financial gain are a few of the top reasons why cyberattacks are conducted on both large and small organizations, especially the federal government. Two main reasons why organizations struggle with cyber defense are low cybersecurity awareness and lack of skilled personnel.

These labs aim to further educate users on how cyberattacks are commonly conducted and what organizations can do to reduce their risk and secure their systems from being compromised. The labs are split into two separate parts: offensive security, referred to as the red team, and defensive security, referred to as the blue team. The red team labs are designed to educate users on the tactics, techniques, and procedures that are utilized in successful cyberattacks throughout the cyber kill chain. The blue team labs will enable users to understand how systems can be configured and secured which will help mitigate the risk of a successful attack, similar to those demonstrated in the red team labs. These hands-on labs are a tactile method to provide users the ability to develop strategies and processes for defending their organization and its systems to ensure data security, customer confidence, and financial growth.

- Hands-on Lab environment to display the importance of cyber defense through use of the Lockheed Martin Cyber Kill Chain (CKC)
- Provide hands on experience with cyber-attacks through exploitation of the attack surface
- Present users with DoD Cyber tools used to assist in cyber defense operations

Pre-workshop Tutorials

A full description and fees associated with these courses are located on the website

Tuesday, October 18 – Morning Sessions (8:00 a.m. to 12:00 p.m.)

Cybersecurity Assessment of MIL-STD-1553 (Coast B)
Adam McCorkle, Georgia Tech Research Institute

A Process for Distributed LVC in T&E (Coast D)
Michael O'Connor, TRIDEUM Corporation

Introduction to Cyber Resilience Test and Evaluation (Coast E)
Jean Petty, Cyber Resilience T&E Manager, Department of Homeland Security (DHS)

Tuesday, October 18 – Afternoon Sessions (1:00 p.m. to 5:00 p.m.)

Cybersecurity Solutions with JMETC, TENA, and TRMC BDA (Coast A)
Gene Hudgins, TENA/JMETC, KBR

ARCUS Cloud – Cyber Tools and Ranges (Coast D)
Peter Walsh, Jackpine Technologies Corp.

T&E in a Digital Engineering Environment (Coast E)
Jean Petty, Cyber Resilience T&E Manager, Department of Homeland Security (DHS)

Agenda

Wednesday, October 19

8:00 a.m. to 8:30 a.m.	**Opening Ceremony and Welcome** (Coast C)
	Shelby Pearce, Program Chair **Bruce Einfalt**, Chairman of the Board, ITEA **Andy Overbay**, Technical Chair
8:30 a.m. to 10:00 a.m.	**Keynote & Featured Speaker**
8:30 a.m. – 9:15 a.m.	**James Wells** (SES), Director Office of Test and Evaluation, Department of Homeland Security (DHS)
9:15 a.m. – 10:00 a.m.	**Brig Gen Rawls**, Commander, Air Force Operational Test and Evaluation Center (AFOTEC)
10:00 a.m. to 10:30 a.m.	**Refreshments** (Atrium)
10:30 a.m. to 12:30 p.m.	**Featured Speakers Continued**

A Change to the Agenda!

10:30 a.m. – 11:15 a.m. **Sarah Standard**, Cybersecurity Technical Director, OUSD R&E, Developmental Test, Evaluation, and Assessments (DTE&A)

A Change to the Agenda!

11:15 a.m. to 12:15 p.m. **Lunch** (Calypso Café Atrium)

12:15 p.m. – 1:00 p.m. **George Rumford**, (SES) Director (acting) and Principal Deputy, Test Resource Management Center (TRMC)

1:00 p.m. to 3:00 p.m. **Hands-on Lab Experience and Technical Exchange**

Session: Hands-on Lab (Coast E)
Join us for a 7-phased hands-on approach to a Red Team Attack and Blue Team Countermeasures Concept where the Red Team and Blue Team would be you the attendee guided by Cyber SMEs who are providing a technical overview, expertise, and insight into the 7-phases.

Session: Technical Exchange and Roundtable (Coast D)
Join us for an open technical exchange on strategies, challenges, and solutions with our Corporate Members and Sponsors. More information to follow.

3:00 p.m. – 3:15 p.m. **Refreshments** (Atrium)

3:15 p.m. – 5:15 p.m. **Technical Sessions** (Running concurrently in Coast A, B, D, E)

Session 1: Cybersecurity Test Technology (Part 1) (Coast A)
Chair: **Min Kim**, Deputy Executing Agent for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

Start Time	Author(s)	Presentation
3:15 p.m.	Dr. Mike Shields, TRMC T&E/S&T and Pete Firey, MITRE	*Measure and Share: TRMC T&E/S&T Cyberspace Test Technology's project to improve Cyber T&E impacts across DoD*
3:45 p.m.	Steve Durst, Terry Champion, Eric Renouf, Skaion	*Activity and Content Enhancement – Next Gen Traffic Generation Toolkit*
4:15 p.m.	Terry Patten, Gerald Fry, David Kelle, Brian Gzemski, and Bradley Mahan, Charles River Analytics	*The Future of Cyber Monitors*
4:45 p.m.	Dr. Himanshu Upadhyay, Dr. Leonel Lagos, Santosh Joshi, Jayesh Soni, and Michael Perez, Florida International University	*Automated Machine Learning for Cyber Security*

Session 2: Securing the SW Supply Chain and Infrastructure (Coast B)
Chair: **Pete Crump**, Georgia Tech Research Institute

Start Time	Author(s)	Presentation
3:15 p.m.	Michael D Brown, Trail of Bits	*Automated Tools for Securing the Software Supply Chain – pre-recorded*
3:45 p.m.	Michael House, DESE Research Inc.	*Attack Surface Reduction through Binary Analysis*
4:15 p.m.	John Peace, FAA	*Cybersecurity Data Science (CSDS) for the Aviation Ecosystem*
4:45 p.m.	Melissa Glazener, Taylor Mitchell, Joey Mink, Reggie Johnson, Ricoh Glover, Ian Doull	*Platform Thinking: Bridging the Warfighter Gap with DevSecOps*

Session 3: Test Design, Regulations, and Best Practices (Coast D)
Chair: **M. John Rafferty**, USAF

Start Time	Author(s)	Presentation
3:15 p.m.	Steven Newton, Sarah Standard	*DoD Cyber T&E Cyber Focus Chapter and Companion Guide Deep Dive*
3:45 p.m.	Gilmore, Avery, Girardi, Medlin	*Applying Design of Experiments (DOE) to Cyber Testing*
4:15 p.m.	Steve Millar	*DevOps to DevSecOps: Making Security Part of Your Development Operations*
4:45 p.m.	Steve Seiden, Acquired Data Systems	*Cybersecurity in the Operational Technology (OT) World*

5:30 p.m. to 7:00 p.m.	**Join us for a Networking Reception** (Atrium)

Thursday, October 20

8:00 a.m. to 8:15 a.m.	**Welcome & Review of the Day** (Coast C)

8:15 a.m. to 10:30 a.m.	**Featured Speakers**
8:15 a.m. – 9:00 a.m.	**Maj Gen Evan C. Dertien**, Commander, Air Force Test Center, Edwards Air Force Base
9:00 a.m. – 9:45 a.m.	**AJ Pathmanathan**, Director, National Cyber Range Complex
9:45 a.m. – 10:30 a.m.	**Joe Bradley**, Executive Director of the Cyber Resiliency Office for Weapons Systems (CROWS)

10:30 a.m. to 11:00 a.m.	**Refreshments** (Atrium)

11:00 a.m. to 12:30 p.m.	**Featured Speakers**
11:00 a.m. – 11:45 a.m.	**Col William E. Young, Jr**., PhD (USAF Ret) Former Commander, 350th Spectrum Warfare Wing
11:45 a.m. – 12:30 p.m.	**Col. David Hoffman**, Commander, 96th Cyberspace Test Group

12:30 p.m. to 1:30 p.m.	**Lunch** (Atrium)

1:30 p.m. to 3:00 p.m.	**Technical Sessions running concurrently and Hands-on Lab Experience**

Session 4: Best Practices for Cyber Evaluation Tools (Coast A)
Chair: **Ryan Christiansen**, AFMC, 412 TENG/JT4

Start Time	Author(s)	Presentation
1:30 p.m.	Megan Fischer, AFMC	*Security Impact Analysis and Risk Management Boards (cyber-evaluation tools)*

2:00 p.m.	Megan Fisher; Todd Jacob, Ryan Christiansen, Evan Thomas	*Reducing the Burden of a Cyber Table Top (CTT-LITE)*
2:30 p.m.	Megan Fischer	*CTT to RMF (part of the analysis process for the CTT)*

Session 5: Assessing and Mitigating Risk (Coast B)
Chair: **Jeremy Werner**, PhD., ST, OSD, DOT&E, Strategic Initiatives, Policy & Emerging Technologies

Start Time	Author(s)	Presentation
1:30 p.m.	William D. Bryant	*Unified Risk Assessment and Measurement System*
2:00 p.m.	Dr. S. Sarathy; M. Marquez, T. Ngo, J. Goh, Dr. S-k Chin, Dr. Q. Qiu, Dr. W. Young	*Hybrid Assurance Approach for Hardware Based MLS Security*
2:30 p.m.	Michael Kaplan	*LOOKOUT: Low-Overhead Observations Keeping Operational Under Threat*

Session: Hands-on Lab Experience (Coast E)
Join us for a 7-phased hands-on approach to a Red Team Attack and Blue Team Countermeasures Concept where the Red Team and Blue Team would be you the attendee guided by Cyber SMEs who are providing a technical overview, expertise, and insight into the 7-phases.

3:00 p.m. to 3:15 p.m.	**Refreshments** (Atrium)

3:15 p.m. to 5:15 p.m.	**Technical Sessions running concurrently** **Hands-on Lab Experience**

Session 6: Cybersecurity Test Technology (Part 2) (Coast A)
Chair: **Min Kim**, Deputy Executing Agent for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

CUI [Controlled Unclassified Information (CUI) session] This one track will have limited participation to U.S. citizens who are employees of the U.S. Federal Government or its contractors (C), or employees of the Department of Defense or its contractors (D). If you do not meet this requirement, you will be unable to attend this one track. DoD common access cards (CAC) or personal identity verification (PIV) will be required for entry. After the one track – the session will be open to all attendees.

Start Time	Author(s)	Presentation
3:15 p.m.	Susi McKee and Brad Mahan, 47th Cyberspace Test Squadron / OL-A	** CUI * NSITE (Network, System Integration and Test Environment) – CTC (Cyber Test Capabilities)*
3:45 p.m.	Arch Owen, Draper – National Security and Space	*Vader Modular Fuzzer: What, Why and How*
4:15 p.m.	Andrew Shaffer, & Bruce Einfalt	*Automated Attack Framework for Test & Evaluation (AAFT)*
4:45 p.m.	Dr. Himanshu Upadhyay, Dr. Leonel Lagos, Santosh Joshi, Jayesh Soni, and Steven Valle, Florida International University	*Cyber Threat Automation & Monitoring System*

Session 7: Future of Test (Coast B)
Chair: **William L'Hommedieu**, COLSA

Start Time	Author(s)	Presentation
3:15 p.m.	Leonard Moskal	*Update from the Executive Agent for DoD Cyber Test Ranges*

3:45 p.m.	Tilghman Turner; Michael O'Connor, Ken LeSueur	*Virtual Blockhouse for Remote T&E*
4:15 p.m.	Brian Pate, Davis, Durr, Conway	*SpaceCREST*
4:45 p.m.	Michael J. O'Connor; Brett Boren, Ken LeSueur	*A Hybrid Digital Twin for T&E*

Session 8: Cybersecurity Testing (Coast D)
Chair: **Leslie 'Duke' Himebrook**, 346th Test Squadron

Start Time	Author(s)	Presentation
3:15 p.m.	Lonnie Becnel, Research and Engineering Services Technical Lead	*Introduction to the National Cyber Range Complex - Unclassified*
3:45 p.m.	Cortney Ferguson, 346th Test Squadron	*346th Cybersecurity Assessment Capabilities*
4:15 p.m.	Lt Col Adan "Face" Reyes, 346th Test Squadron	Operational Test and Cyber Test in an agile software development environment
4:45 p.m.	Lt Col Adan "Face" Reyes, 346th Test Squadron	Operational Test and Cyber Test in an agile software development environment

Session: Hands-on Lab Experience (Coast E)
Join us for a 7-phased hands-on approach to a Red Team Attack and Blue Team Countermeasures Concept where the Red Team and Blue Team would be you the attendee guided by Cyber SMEs who are providing a technical overview, expertise, and insight into the 7-phases.