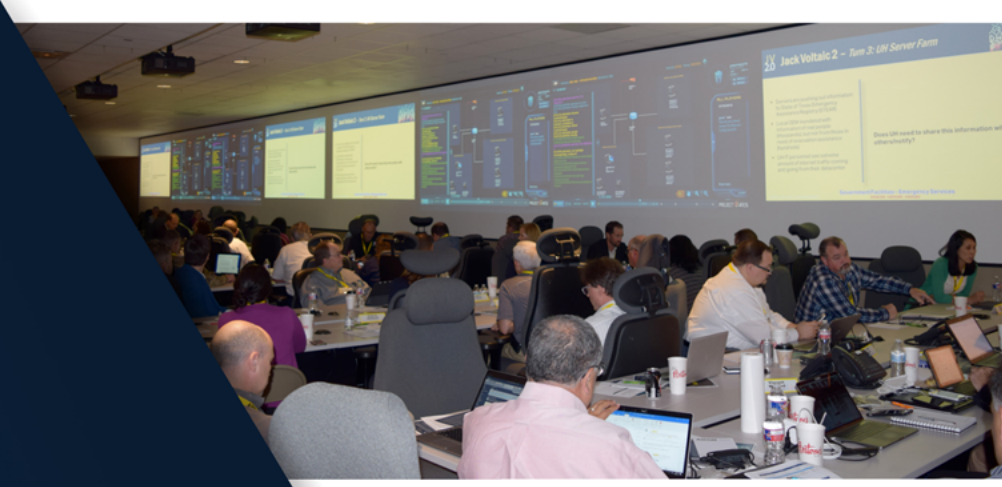
CIRCADENCE

STATE & LOCAL GOVERNMENT CYBER TRAINING

Live Fire Security Readiness Emerges at Jack Voltaic 2.0



ABOUT THE EVENT

Public and private government entities and critical infrastructure organizations came together in the summer of 2018 to participate in the Jack Voltaic 2.0 Cyber Research Project -- an cyber resiliency collaboration that examined a city's ability to respond to a multi-sector cyber attack.

Hosted by the **City of Houston** in partnership with **AECOM** and **Circadence**, the project assembled state and local government partners to assess incident response procedures. Developed by the **Army Cyber Institute at West Point**, Jack Voltaic 2.0 built upon their understanding of existing cyber security capabilities as well as protection gaps.

Circadence provided its immersive cyber security learning platform, Project Ares®, to support the exercise. The Army Cyber Institute used the results of the exercise as a preparation framework for municipalities throughout the United States . A summary of findings and recommendations was published here.

PROJECT ARES CONTRIBUTION TO SUCCESS

- Teams were immersed in the scenarios with Project Ares virtual environments.
- Participants were engaged and treated the experience as 'real'.
- Combination of live fire and table top exercises improved participant's communication and made the learning experience persuasive.

OUTCOMES AND OBSERVATIONS

- Project Ares received positive feedback from life fire exercises (LFX) players, table top exercises (TTX) players, observers, distinguished visitors and JV2 coordinators.
- The event was highly relevant for all exercises of this nature and could be replicated in other LFX for municipalities.
- The ability to provide LFX and TTX game play with real-time discussions between players was a value add to attendees.

PROJECT ARES CYBER MISSIONS UTILIZED AT JV2

Mission 4, Operation Arctic Cobra

Cyber defenders analyzed network traffic and stopped a malicious exfiltration process.

Mission 5, Operation Wounded Bear

Cyber operators identified and removed malware responsible for identity theft and protect the network from further infections.

Mission 6 Operation Angry Tiger

Cyber operators conducted a risk assessment of a company's existing network structure and its cyber risk posture for possible phishing attacks.

- CenterPoint Energy participated in this exercise.

Mission 8, Operation Ocean View

Cyber operators conducted an incident response mission for a water treatment plant's infrastructure to include the SCADA systems.

- The Cyber National Mission Force participated in this exercise.

Mission 10, Operation Crimson Wolf

Acting as a cyber force member, players had to stop ransomware from spreading/infecting other boxes on the network.

- The Port of Houston Authority, Memorial Hermann, and Harris Health System participated in this exercise.

Mission 12, Operation Bold Hermit

Cyber defenders had to identify reconnaissance activity and beacons inside the network and locate the attack vector. They also had to implement instrusion detection capabilities to eliminate attack-associated activity.

- The University of Houston, Harris County Information Technology Center, Blue Lance, and Houston Information Technical Services

PROJECT ARES®

Project Ares is an immersive, gamified cyber security learning and assessment platform running on Microsoft Azure that helps state and local government agency cyber professionals keep their skills sharp.

SCHEDULE A DEMO TODAY

303.413.8800 • www.circadence.com • sales-cyber@circadence.com

HEADQUARTERS Boulder, CO 80302
ADVANCED RESEARCH & DEVELOPMENT FACILITY Tupelo, MS 38804
CENTER FOR CYBER AUTONOMY San Diego, CA 92123
WASHINGTON D.C. SALES McLean, VA 22101

CIRCADENCE