CYBER FLORIDA
AT THE UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH

Jack Voltaic™ (JV) Tampa
AAR Brief to FRWA

Bruce D. Caulkins, Ph.D.
caulkins@cyberflorida.org

29 June 2026

Cyber Florida:

The Florida Center for Cybersecurity was established by the state legislature (Chapter 1004.444) in June 2014 (updated in 2024) to "**position Florida and its related workforce as a national leader in cybersecurity through education, research, and community engagement**."

What does Cyber Florida do?

- Conduct research projects to assist in cyber workforce development and training across the state
- Assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce
- Act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training
- **Seek out partnerships with major military installations** to assist, when possible, in homeland cybersecurity defense initiatives
- Attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors

WHAT ARE WE DOING?

GRANT-FUNDED & STATE INITIATIVES

Florida's Cybersecurity Critical Infrastructure Risk Assessment

Conduct a voluntary cybersecurity risk assessment for Florida-based public and private critical infrastructure organizations

Statewide Cybersecurity Training Program

Provide cybersecurity awareness and training courses tailored to job roles for all public-sector employees

Cyber Range (HB 5001)

Provide a cost-effective, realistic cybersecurity training environment for city, county, and local governments

CyberWorks: Cybersecurity Workforce Development (NCAE)

Prepare veterans and transitioning first responders for jobs in cybersecurity

WHAT ARE WE DOING?

ONGOING PROGRAMS

Operation K12

Infuse cybersecurity awareness and career preparation throughout the Florida education system

Seed Fund Pilot Program

Supports Florida-based researchers and emerging entrepreneurs in commercializing their cybersecurity technical innovations, launching new businesses, and helping secure critical infrastructure

Policy & Research

Fund and facilitate research and help guide public policy by educating both the decision-makers and the public on best practices and policy initiatives

SOCAP: Security Operations Center Apprentice Program

Provide hands-on experience to complement degree programs and services to support the public sector

Security Operations Center Apprentice Program

Provides hands-on cyber threat monitoring, digital forensics, and reporting skills for up to 20 USF students each year

SERVICES OFFERED/STUDENT LEARNING OBJECTIVES

- Digital forensics, including enterprise and mobile devices
- Incident response (remote triage assistance)
- Malware analysis
- Log management and review/log collection and analysis
- Cybersecurity projects, assessments, and consulting
- Coming soon: vulnerability assessment and penetration testing

Cyber Ranges

What are Cyber Ranges?

Cyber ranges are simulated networks that:

- Provide an interactive representation of an organization's technological assets
- Allow users to develop and train their cybersecurity skills in a safe and controlled environment
- Provide performance-based learning and assessment
- Provide environment where teams can work together to improve teamwork and team capabilities
- Garner real-time feedback
- Allow a simulation of on-the-job experience
- Provide an environment where new ideas can be tested, and teams can work to solve complex problems
- Provide individual or team-based training and exercises

Commercial vs. Open Source

Commercial Pros:

- Costs handled by company
- Hardware purchases not needed locally
- Higher quality of training
- LMS embedded in system
- Red team enabled environments

Commercial Cons:

- High costs
- Content control can be an issue
- Dependent on network

Open-Source Pros:

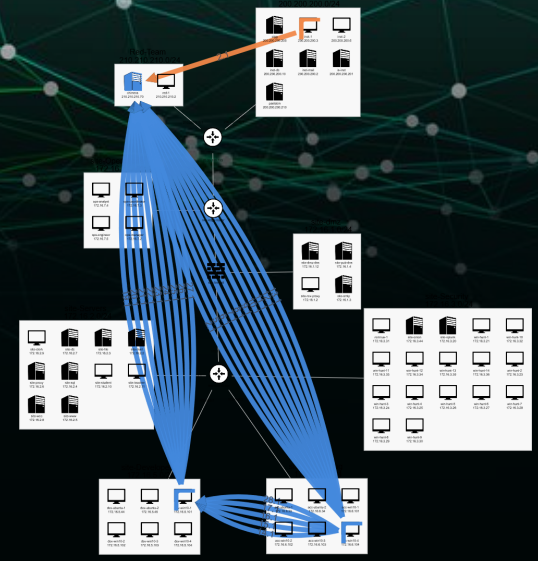
- Lower costs, in general
- Greater control of content and direction of training
- Flexible

Open-Source Cons:

- All costs on host organization – hardware, licenses
- LMS needed
- Red team members' costs

In 2022-2023, Cyber Florida looked at acquiring a cyber range…

What does Cyber Florida need in a range?



- → A virtual environment designed to **simulate real-world cyber scenarios for training, testing, and experimentation**
- → Allows cyber professionals to practice defending against attacks, test systems, and develop skills in a safe, isolated setting with commercial tools
- → These ranges replicate networks, systems, and threats to provide hands-on experience without risking actual infrastructure

Aligned Realistic Cyberattack Simulation (ARCS) Range

powered by CYBER FLORIDA AT USF + SIMSPACE

ARCS RANGE

ALIGNED REALISTIC CYBERATTACK SIMULATION RANGE

RANGE FEATURES

- Florida County and Local government IT and cybersecurity personnel - **public sector focused**
- Cyber Range as a Service (CRaaS), 100% cloud-based training model
- No cost for users
- Supports Annual CSIRT Training for 34 state agencies
- Supports AI and OT/ICS sectors

KEY MILESTONES

- ✓ Dec 2023: SimSpace contracted to provide services
- ✓ Currently 3,928 users across 41 counties on range
- ✓ Executing conference competitions – FLGISA, CyberBay
- ✓ Supports cyber LFXs like Jack Voltaic, and CTFs like Cyber Launch, and Congressional App Challenge

ARCS Cyber Range:

- A hyper-realistic platform for both offensive and defensive cybersecurity training for IR teams and individuals. The platform is equipped with real-world simulations of complex networks and systems, enabling users to engage in practical exercises that mirror current cyber threats.

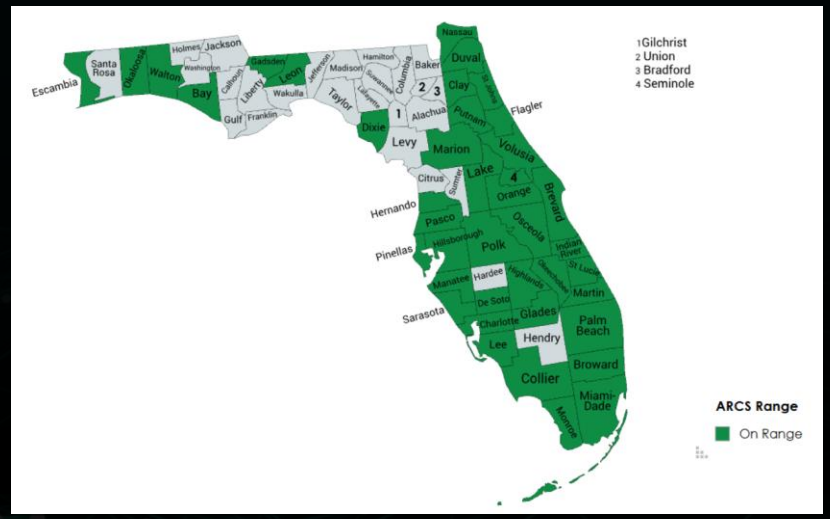
powered by CYBER FLORIDA AT USF + SIMSPACE

ARCS RANGE

ALIGNED REALISTIC CYBERATTACK SIMULATION RANGE

ARCS Range began Dec 2023 – 3 year contract with SimSpace

- ***Nearly 4,000 users, covering 41 counties, focused on public sector in FL – no-cost training to users***
- ***Focused on individual training (asynchronous) and team exercises (synchronous)***
  - ✓ Conducted required 4-hour assessments separately for 32 state-level departments' CSIRTs with FL[DS] and IG (‘24 and ‘25)
  - ✓ Conducted range support for Jack Voltaic LFXs
  - ✓ Executed FLGISA Winter Symposium cyber range competition
  - ✓ Hosted several international delegation visits to USF (CENTCOM-led events) and in Bahrain
  - ✓ Supporting USF NIST and DoE Research projects
  - ✓ Executed Sunshine Cyber Conference cyber competition

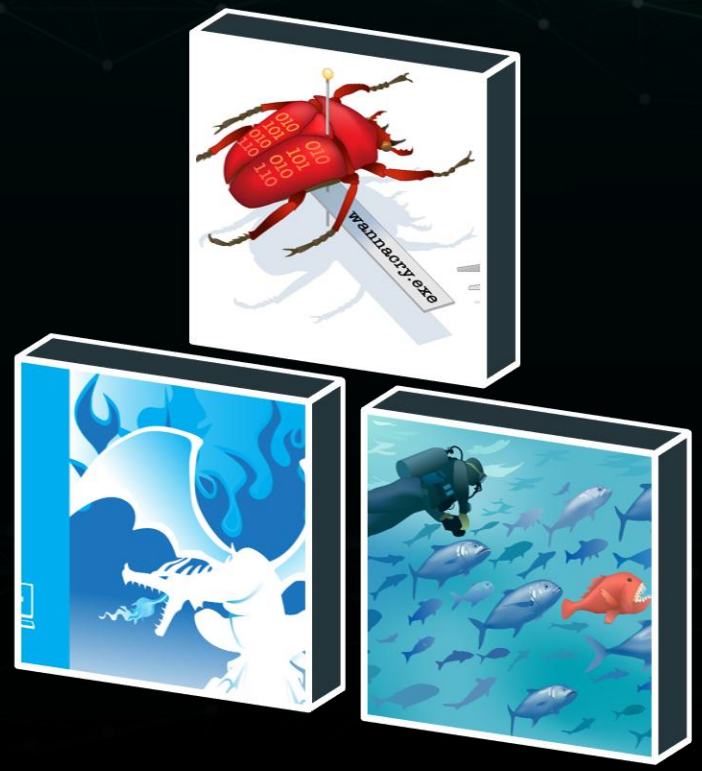


Training Modules:

- **Structured, modular training content** with interactive tutorials, quizzes, and hands-on exercises to reinforce learning.

Features:

- **Provides targeted learning paths** based on individual, or team needs to allow for systematic skill development from basic to advanced levels.
- **130+ Individual training modules** which are available on-demand and span the following areas:
  - SOC Analyst
  - Threat Hunting
  - Forensic Analyst
  - Malware Analyst
  - Vulnerability Assessment
  - Threat Intel
  - Application Security
  - Red Teaming
  - SIEM Analyst
  - Incident Response

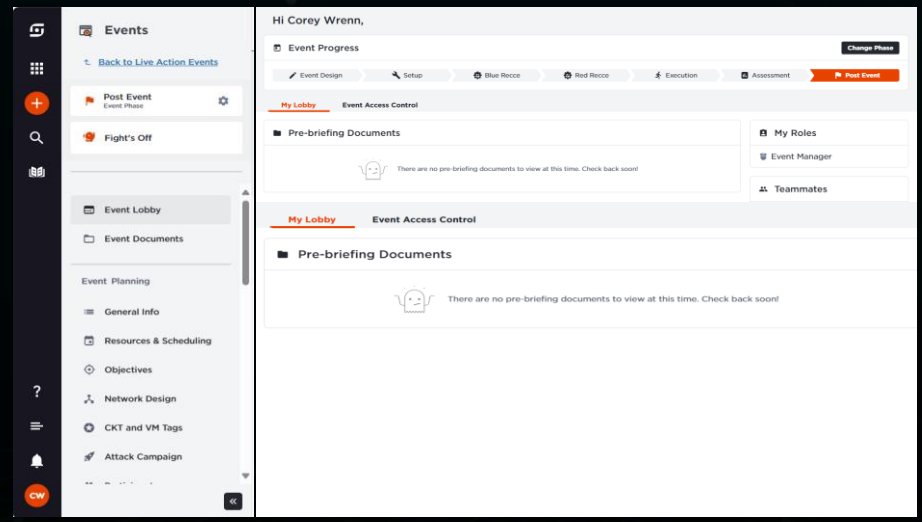


Live Action Event:

- **An interactive experience that prepares your team** to handle real-world cyber attack scenarios with confidence.

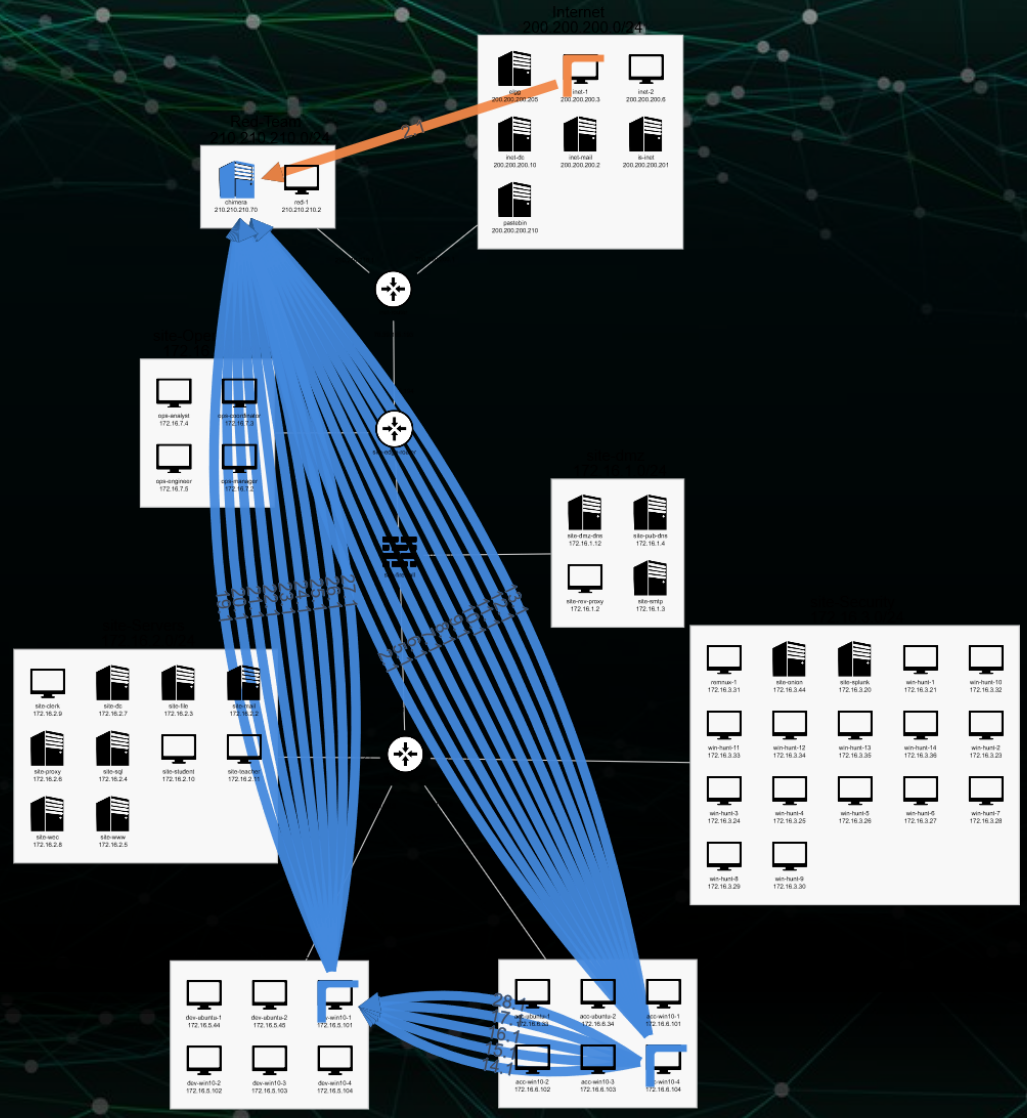
Features:

- **Simulate an array of realistic attack scenarios** to simulate a dynamic range of cybersecurity threats and incident types for your team to perfect detection, analysis, and response.
- **Collaborative training environments** for remote and distributed teams during team-based exercises for multiple users to work together to resolve simulated incidents.
- **Scalable infrastructure, customizable environments, and scenarios** to support a range of users from small teams to large organizations and accurately reflect the organization's networks and threat landscape.



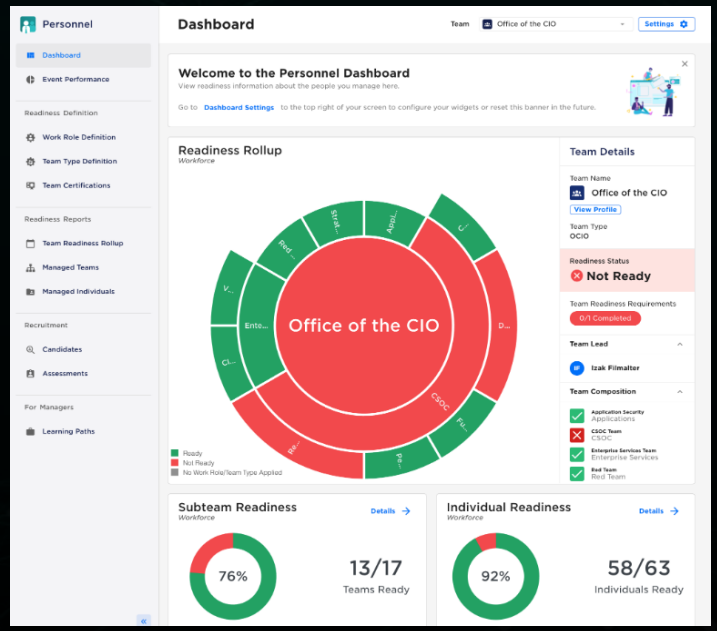
ARCS Cyber Range In Action:

- **Red Team / Blue Team Exercises**: Engage in realistic, adversarial training scenarios to strengthen both offensive (Red Team) and defensive (Blue Team) skills.
- **Capture The Flag (CTF) Challenges**: Interactive competitions that help participants develop problem-solving skills across a range of cybersecurity topics, such as penetration testing, malware analysis, and vulnerability exploitation.
- **Custom Scenarios**: Tailor scenarios to replicate specific organizational systems, threat landscapes, or attack methodologies.



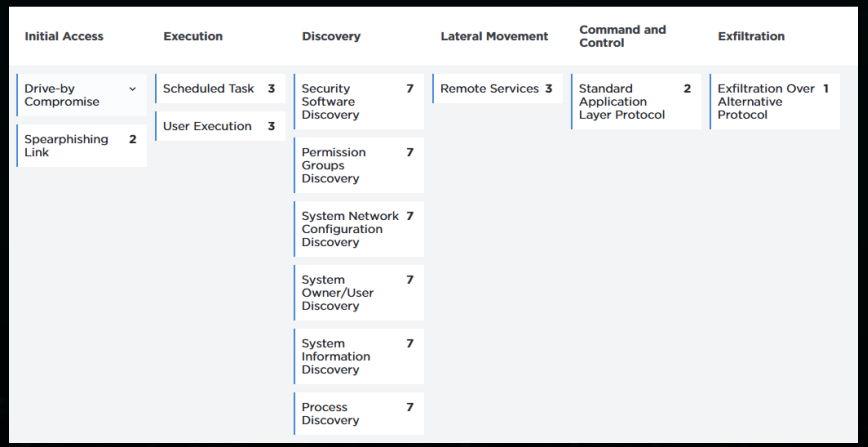
ARCS Cyber Range Benefits:

- **Enhances teamwork and communication skills** for effective cybersecurity operations, improving ability to manage and respond to security incidents.
- **Accelerates the training of junior staff** to the cybersecurity field allowing for faster workforce integration.
- **Prepares cybersecurity professionals for real-world situations** through hands-on practical scenarios and exposes personnel to a variety of attack vector experiences.
- **Generate comprehensive, detailed reports** using performance-based metrics to highlight strengths and areas for improvement for individuals and team performance.



ARCS Cyber Range Benefits (Cont.):

- **Simulate an array of realistic attack scenarios** for your team to perfect cybersecurity operations.
- **Monitor skill progression through different skill levels** and training modules and observe user actions and performance in real-time during training exercises.
- **Flexible access for remote and distributed teams** from various devices and locations.
- **Adaptive threat models based on user performance and skill level** to adjust the complexity and intensity of simulated attacks to systematically drive team maturity.



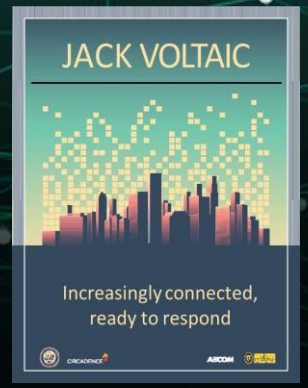
CYBER FLORIDA

AT THE UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH

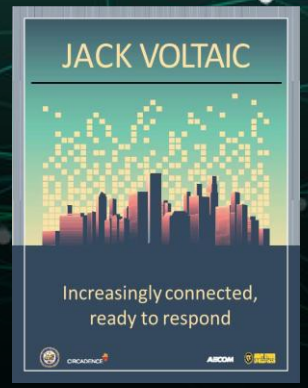
Jack Voltaic™ (JV) Tampa

What is JV?

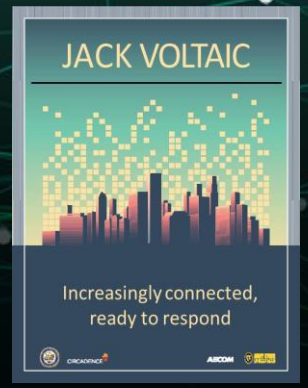


- The JV initiative originated with the U.S. Army Cyber Institute (ACI) at West Point to enhance critical infrastructure resilience through practical, multi-sector cyber exercises.
- Launched in response to growing cyber threats to interdependent systems, it adopted a “bottom-up” approach involving local governments, private industry, first responders, and military partners.
- The program emphasizes civil-military coordination at the community level in unclassified settings to identify gaps in cybersecurity, incident response, and recovery capabilities.

What is JV?



- JV has evolved from a small, single-city experiment (JV 1.0 NYC financial district) into a repeatable, multi-sector research framework (JV 5.0 in Tampa).
- JV 2.0 was a city-wide exercise with the City of Houston, involving 200 participants from 44 organizations across 8 sectors with similar goals & objectives as the JV-Tampa event.
- JV 3.0 expanded to hundreds of distributed participants and delivered back-to-back “fort-to-port” exercises with Savannah, GA and Charleston, SC.

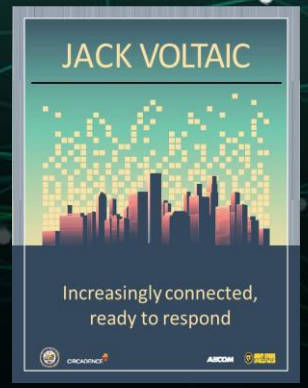


What is JV?

JV 5.0 (Tampa) was a Cyber Florida-sponsored event using TTX and cyber range platforms, focused on multi-sector response to a cyber attack on the water sector, affecting DoD and local govt's.

<u>Core Purpose</u>: JV is a "bottom-up" research experiment designed to identify gaps in critical infrastructure (CI) protection and synchronize Department of War (DoW), government (federal/state/local), and private sector responses to cyber-physical attacks.

JV Tampa’s Objectives



- Exercise the City of Tampa and Hillsborough County’s abilities to respond to a multi-sector, multi-pronged cyber-attack.
- Assess the ability of state and local public-sector entities to respond to these types of attacks in an already-stressed EM environment.
- Showcase the City of Tampa and the surrounding counties as emerging national leaders in cybersecurity, particularly cyber incident response.
- Evaluate and examine the U.S. military’s cyber protection capabilities.
- Evaluate MacDill AFB's ability to partner with local entities to minimize operational impact in the eventuality of a cyber-attack on the city of Tampa's critical infrastructure.
- Identify potential operational impacts for USCENTCOM in the eventuality of a cyber-attack on the city of Tampa's critical infrastructure.

JV Tampa:

A long road of preparation – dozens of meetings leading up to event

JV Tampa:
-- 94 attendees (plus 12 visitors)

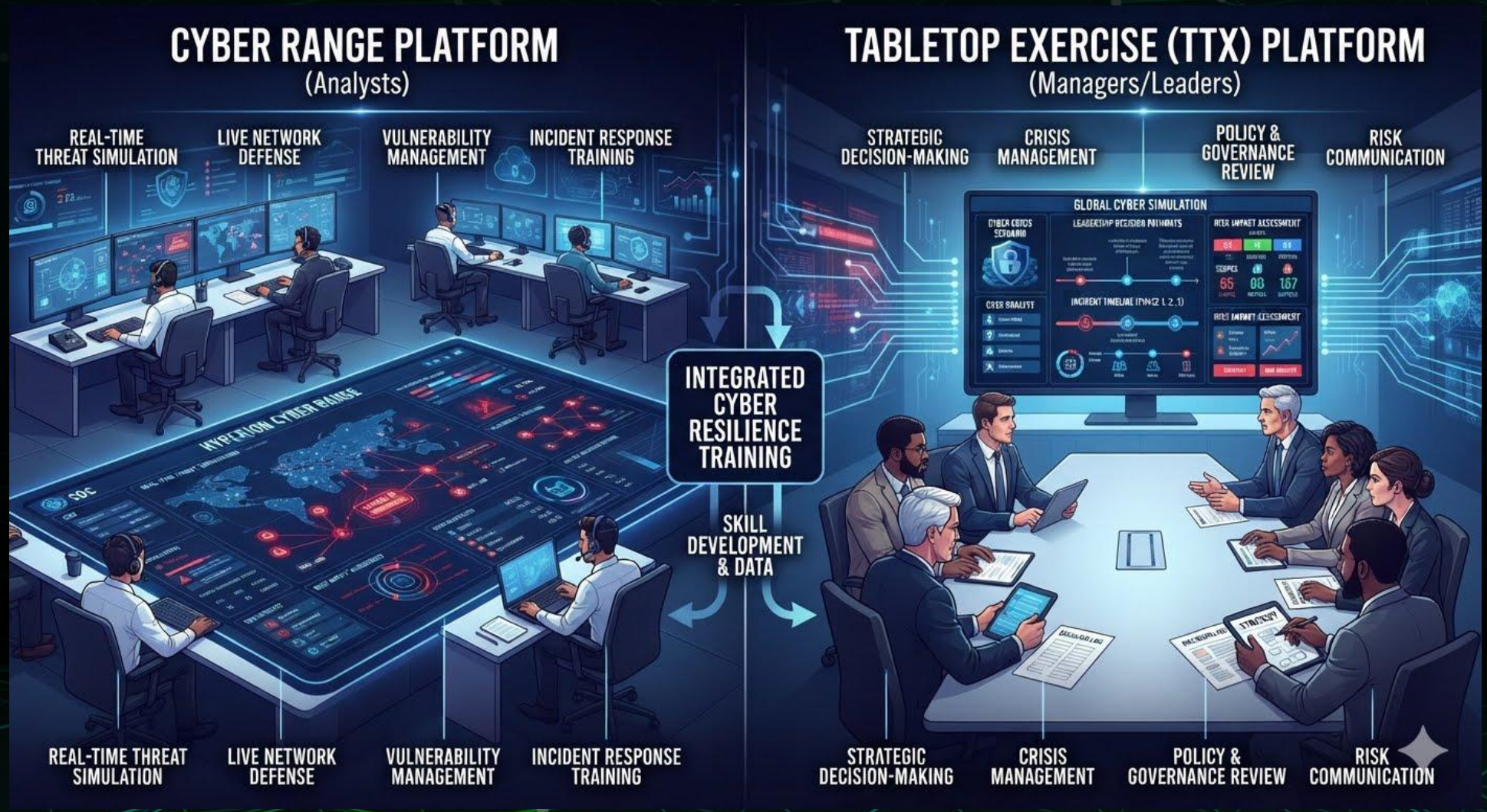
-- 31 organizations

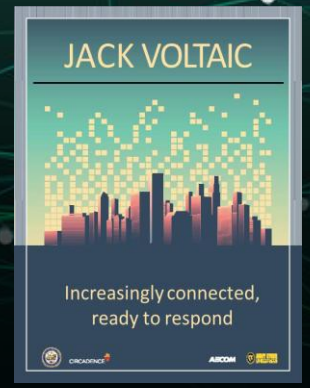
JV Tampa Scenario

The exercise consisted of one scenario – cyber-attack against the water sector in the Tampa area – across two separate platforms – NUARI's DECIDE® platform for the TTX (managerial players) and SimSpace's Cyber Range platform for the LFX (technical players).

Coordination between the two platforms would be achieved via "sneaker networks"; i.e., having LFX team leads brief the TTX participants several times during the exercise day of JV, day 2.

JV Tampa Scenario





Jack Voltaic, Run Against FrostyGoop

A live-fire + table-top exercise modeled on the first ICS malware to weaponize Modbus TCP — the January 2024 attack that cut heat to 600+ Lviv apartment buildings in sub-zero temperatures.

The Threat: FrostyGoop

9th known ICS-specific malware. First to use Modbus TCP (port 502) directly. Downgraded controller firmware, then reported hot-water readings while cold water was pumped — operators flew blind for nearly two days.

Live-Fire Track (LFX)

Technical defenders fought the malware on a closed cyber range — real tools, real telemetry, no risk to production. Modbus traffic, falsified register reads, controller compromise: all played live.

Table-Top Track (TTX)

In parallel, sector leadership and management worked the same scenario at a policy and decision level — the unique value of Jack Voltaic is that both rooms talked to each other.

Sources: Army Cyber Institute (Jack Voltaic); Dragos & Unit 42 reporting on FrostyGoop / BUSTLEBERM (Lviv, Jan 2024)

Practical Exercises Force the Conversation With Management

"Cyber exercises are typically hindered by being either overly technical or too high-level — managers and operators are not in the same room." — Jack Voltaic design principle

Put the SOC and the C-suite in the same scenario.

FrostyGoop is an ICS-protocol attack — a technical detail. Loss of heat to 600 buildings in winter is a business and public-safety decision. The exercise made both groups own the same incident in real time.

Rehearse the translation before you need it.

"Modbus holding-register write to a downgraded controller" means nothing to a VP. "Our sensors are lying to us; the plant is offline" does. Practice that translation under pressure — not during a real outage.

Surface decisions only leadership can make.

Disclose to regulators? Pull internet-exposed PLCs offline and accept downtime? Call the National Guard? The LFX produces the technical signals; the TTX forces leadership to commit to a call — and to a timeline.

Turn lessons into a written escalation playbook.

Every gap exposed — unclear thresholds, missing contacts, slow approval chains — becomes a line item management has now seen with their own eyes. Buy-in for remediation is dramatically easier post-exercise.

Bottom line: the value isn't the malware — it's the conversation it forces between defenders and decision-makers.

Skills Forged on the Live-Fire Range

The LFX wasn't about catching FrostyGoop — it was about building muscle in the three habits every defender needs when the next OT incident hits.

01

Investigative Methodology

- Hypothesis-driven analysis — what would an attacker need to touch?
- Pivoting cleanly from alert → host → user → action
- Mapping observations to MITRE ATT&CK for ICS
- Documenting findings in real time, not after the fact

02

Log Analysis

Proxy
Outbound C2 patterns, beaconing intervals, anomalous user agents

IDS
Modbus traffic on port 502, register writes, signature + anomaly hits

Windows
Event ID correlation, PowerShell history, Sysmon process trees

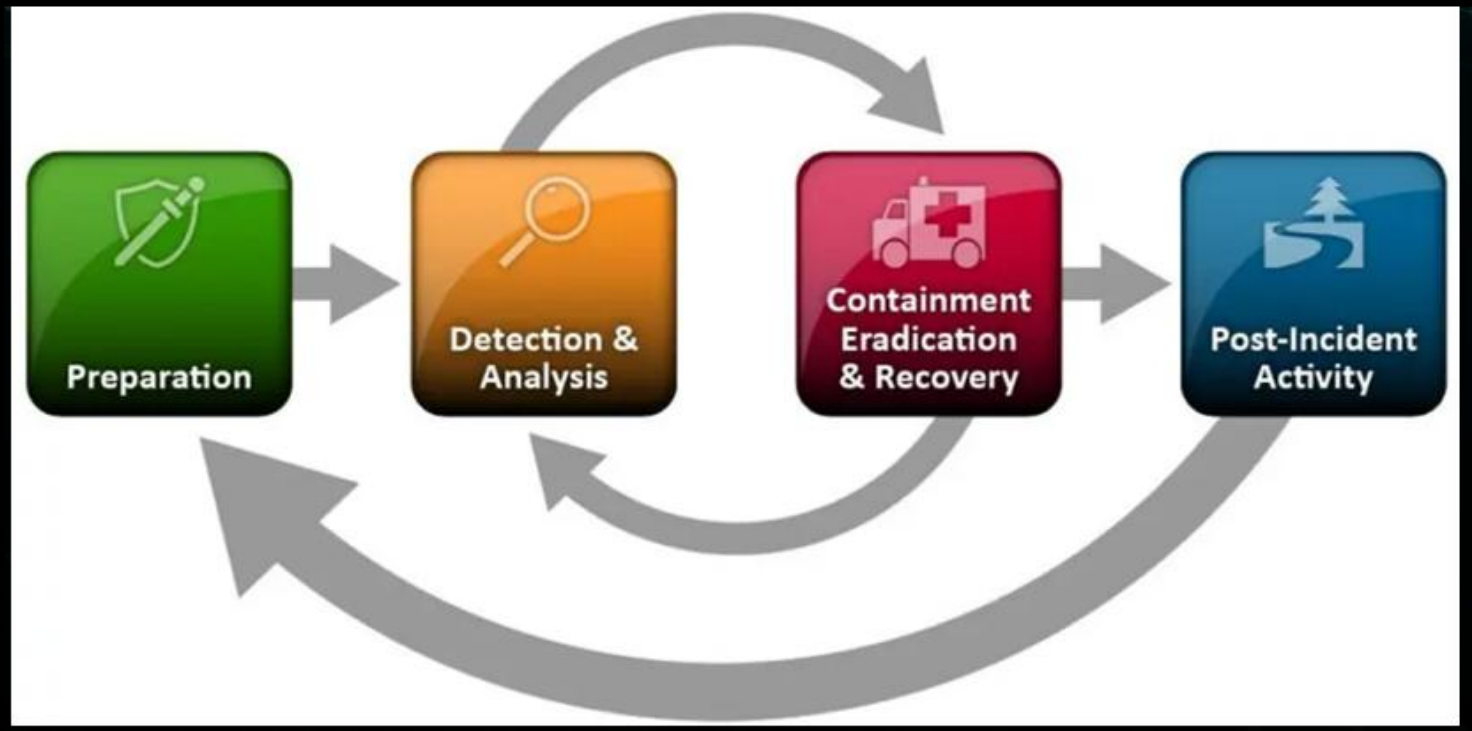
03

Tying It Together: The Story

- Building a single timeline from proxy, IDS, and host data
- Translating Modbus events into business impact
- Briefing technical leads AND non-technical management
- Owning the narrative before someone else writes it for you

Note for incident leads: *Please review this deck for technical accuracy and any redaction requirements before it is briefed externally. Flag attribution language and sensitive controller details for discussion.*

Incident Response Goals



OT Router was accessed externally

Recon was conducted from external

OT Web Server was compromised...
C2 Established.

Internal reconnaissance was conducted

Detection & Analysis

Malicious Administrator creds inserted into registry

Logged in with admin creds to OT Power engineering workstation. Established C2

PLC relay is written to over Modbus.

Physical effects may be occurring

Key takeaways

- **Network is compromised**
  - 4 devices in total compromised
  - C2 established internally
- **Physical effects could be occurring**
  - PLC relays are being written to by the threat actor
- **Creds are compromised**
  - Assume all credentials have been compromised

Mitigations & Remediations

1. **No external, non-approved equipment**
   - Policy
   - Enforcement – shutdown ports, machine certs, 802.1x, rogue sys detection
2. **Micro-segmentation**
   - Logically separate departments, not just networks
   - East/west traffic… deny by default
3. **Active EDR --** *Basic Win 11 Defender management*
   - Defender - block malware, unsigned systems
   - Defender - block unobtrusive PowerShell scripts
4. **Basic Cyber**
   - Webserver lockdown
   - Vulnerability management, scanning, accountability
   - Better security solutions: SOAR, behavioral, AI, single dashboard
5. **OT**
   - Modification alerts

JV Tampa general comments:

* Logistics – rooms were good; needed bigger room for LFX. Food/parking great
* 2 days vs 3 days? Still need 3 but 2 doable
* Briefers were excellent; INL AHA demo was helpful, linked FDLE and FLDS to it
* Needed more “consumers” and CI folks; BUT WE GOT THE RIGHT LFX FOLKS!!
* Having ARCS LFX with TTX provided us excellent insights/feedback
* FL ARNG/USCG participation was key for LFX… and NG told me that they never did exercise like this with civilians/public sector
* FL ARNG folks want to use TTX and ARCS in future (more of an open range event)
* CENTCOM J6 wants to do A&P event at MSC this July (60 pax) with SimSpace
* Do JV Tampa again next year? (sponsors/etc)

QUESTIONS???

CYBER FLORIDA
AT THE UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH