MIDWEST RELIABILITY ORGANIZATION

Maintaining Cyber Resiliency Through Simulation-Based Scenarios

Exercises Specific to the Energy Sector

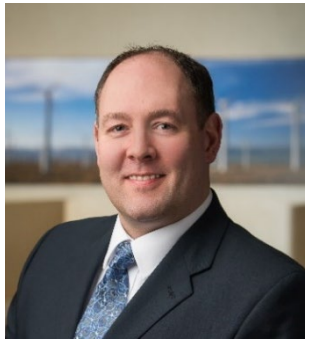
Hosted by MRO and SERC

June 17, 2021

CLARITY | ASSURANCE | RESULTS

Disclaimer

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of MRO.



MIDWEST RELIABILITY ORGANIZATION

MRO

Steen Fjalstad, Director of Security

Steen Fjalstad is the Director of Security for MRO where he coordinates with industry, state, U.S. and Canadian agencies to manage threats & vulnerabilities to the bulk power system.

SERC

SERC

Bill Peterson, Manager, Entity Outreach and Training

Bill Peterson is the Manager, Entity Outreach and Training with SERC Reliability Corporation, a corporation responsible for promoting and improving the reliability, adequacy, and critical infrastructure protection of the bulk power system in all or portions of 16 Southeastern and Central states.

Hosted jointly by MRO and SERC

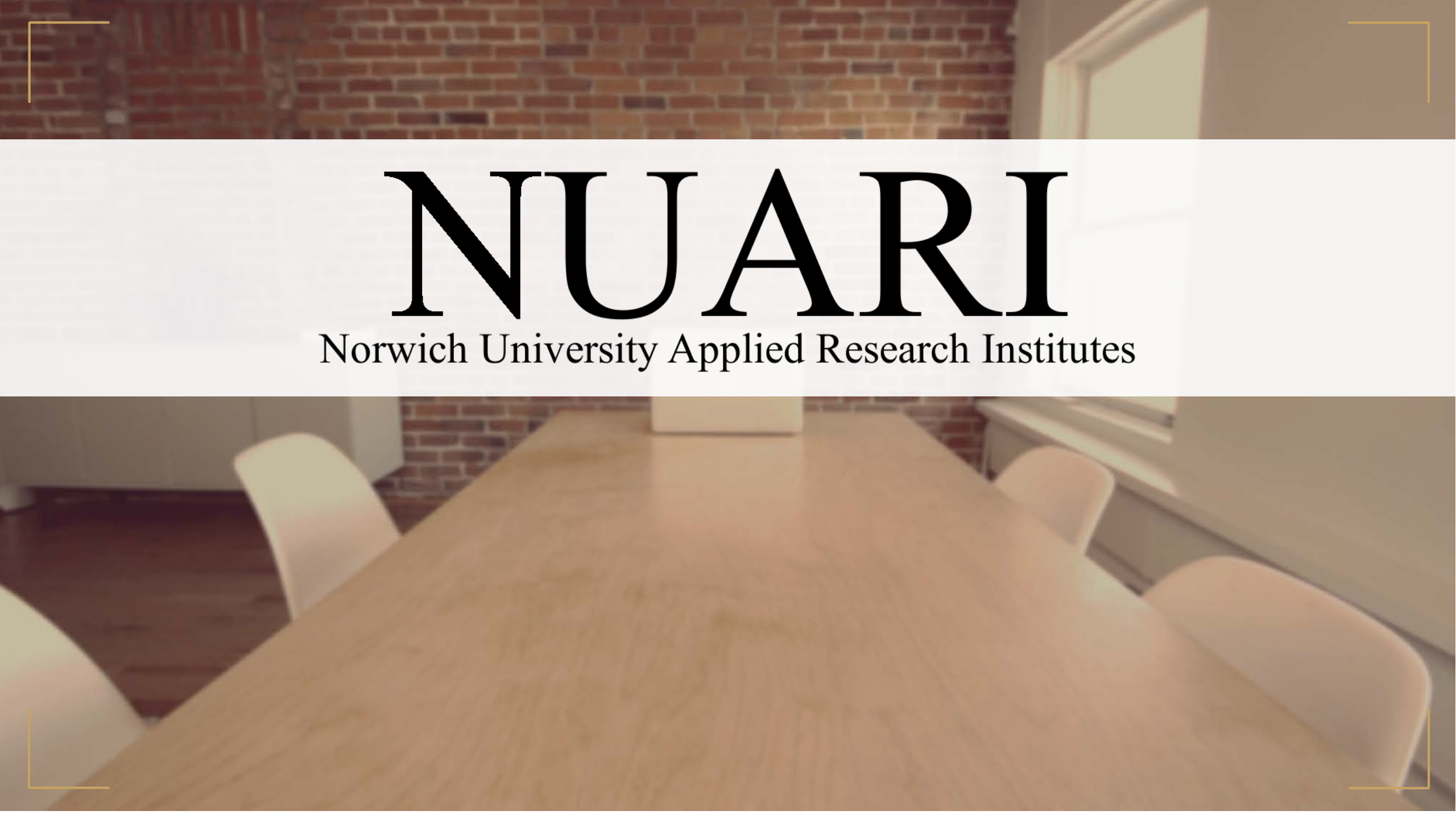
Upcoming Events

SERC

- Summer Regional Meetings on July 20-22, 2021
- Cold Weather Webinar on August 24, 2021
- System Operator Conference on September 14-16, 2021
- Fall Reliability and Security Seminar on October 5-6, 2021
- System Operator November 9-11, 2021

MRO

- MRO SAC Webinar: Consequence Driven Cyber Informed Engineering (CCE) – Resilience Strategies on July 20, 2021
- CMEP Conference on July 27, 2021
- MRO SAC and CMEP Webinar: BCSI in the Cloud - Compliance and Security on August 18, 2021
- Reliability Conference August 24, 2021
- Security Conference and Technical Training on October 4-6, 2021

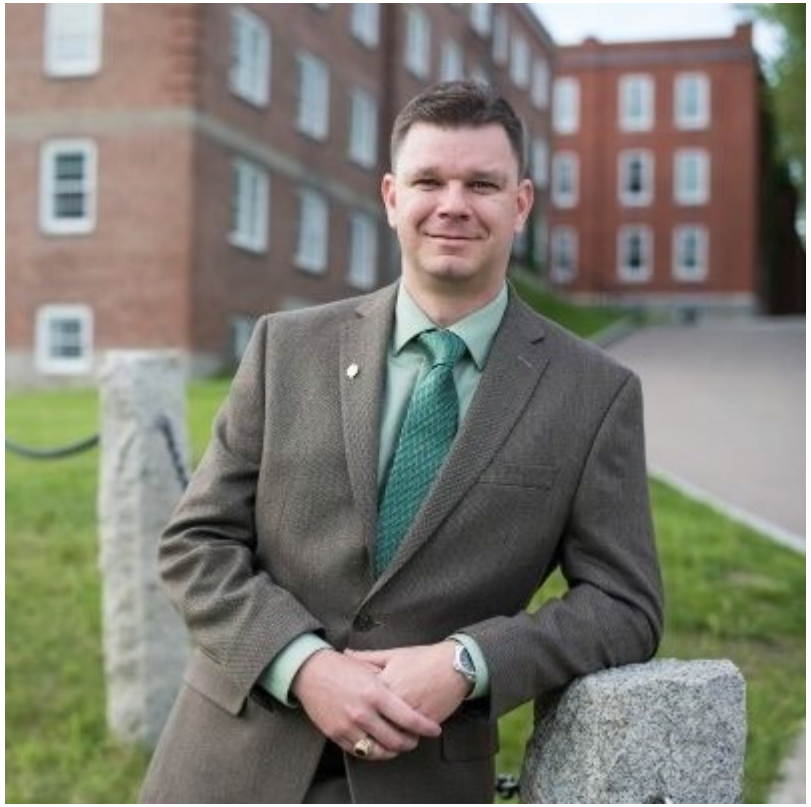


NUARI

Norwich University Applied Research Institutes

NUARI SPEAKERS

Norwich University Applied Research Institutes



Chris Tucker

Cybersecurity Exercise Director

Nathan Reddick

Director of Cybersecurity Outreach

Norwich University Applied Research Institutes

MISSION

NUARI enables a resilient society through rapid research, development, and education in counterterrorism, cybersecurity, defense technologies, and information warfare.

- NUARI is a 501(c)(3) non-profit that serves the nation public interest through the interdisciplinary study of critical national security issues.
- Partially funded by the Department of Homeland Security and the Department of Defense, and federally charter under the sponsorship of Sen. Patrick Leahy.
- Co-located with Norwich University in Northfield, VT, share their ideals of academic excellence, innovation, service to country.

DESIGN TEAM BACKGROUND

Dr. Kristen Pedersen	Tom Muehleisen	Filipp Khosh	Mike Slack	Joe Minicucci
Associate Vice President	**Director of Cyber Research**	**Exercise Planner**	**Exercise Planner**	**Exercise Planner**

WHY EXERCISES?

- Exercise History
  - What value can exercises bring to our operation?
  - Why should we put effort into developing a strong exercise program?
  - Why Simulation-based exercises?

Hurricane Pam Case Study

- Hurricane Pam- An exercise driven planning process that was in progress when Hurricane Katrina struck.

- Consequence modeling results achieved from the exercise planning activities proved to be highly accurate; the only "miss" was in the number of projected fatalities (~2k vs. 60k).

- Credit for the reduction in fatalities is given to the informal knowledge and relationships built during the exercise development and design work that occurred in the months preceding Katrina.

Jack Voltaic Lessons Learned

Exercise Objectives

1. Examine how cyberattacks on commercial critical infrastructure impact Army force projection.

2.Develop a repeatable and adaptable framework that allows cities to exercise their response to a multi-sector cyber event.

3. Exercise the Cities of Charleston and Savannah in emergency cyber incident response to ensure public services and safeguard critical infrastructure.

4. Reinforce a "whole-of-community" approach in cyber incident response through sustained partnerships across industry, academia, and government.

- 130-150 users each day
- 104 injects with data collector notes
- 8 hours of exercise play, generating:
- 869 chat messages to 101,436 participants in 17 chat groups
- 78 questions asked
- 84 sets of answers (players/DC's)

decide®
PLATFORM

Incident & Emergency Response Planning

- Cybersecurity threats - Ransomware, DDoS, etc
- Physical Threats
- Crisis Communication Planning
- Business Continuity Planning
- Power Outages
- Emergency/Disaster Response Planning
- Natural Disasters/Extreme Weather
- COVID-19 & Geopolitical Events

DECIDE Overview Video ← Click Here

Developed with funding from the Department of Homeland Security, the DECIDE platform has been a trusted cybersecurity live exercise solution for more than ten years.

- DECIDE equips organizations, critical infrastructure sectors, the military, and the government with the situational awareness, strategic communications capabilities, and digital response playbooks need to prevail against serious cyber threats.

- DECIDE brings actors from across sectors, geographies, and roles together into a distributed environment to participate in critical infrastructure exercises.

CAPABILITIES OF DECIDE®

- A web-based platform that is used to help facilitate exercises in a virtual and distributed manner
- Ability to create realistic scenarios that are unique to each participating organization, using a system dependencies model & process flow interactive simulation
- Engages all levels of an organization
- Incorporates supply-chains & organizational 3rd party partners to participate and help simulate systemic risk
- Rapid scenario development, modification, and reuse capability
- Automatic data capture of exercise events and player actions
- Real-time performance assessment
- AARs and executive briefs for future action
- Allows participants to validate operational readiness and execute roles/responsibilities

DECIDE Exercise

Current 11:45 AM Mar 15, 2017

Next 11:59 AM Mar 15, 2017

New Messages!

New Questions!

Communic

INBOX 6 | BROADCAST | CHAT

Select All | New | Mark Read

From : Trading Operations
To: Demo Controller Org (Demo Controller)
3/15/17 11:12 AM New
Ransom Non-Payment

From : ACME Information Technology Services
To: Demo Controller Org (Demo Controller)
3/15/17 10:16 AM New
Network Malware Warning

From : Chief Executive Officer
To: Demo Controller Org (Demo Controller)
3/15/17 8:52 AM New
Computer Virus??

From : Equity Trading Associate
To: Demo Controller Org (Demo Controller)
3/15/17 8:19 AM New
Screen Lock Issue - URGENT !!

Sent: **3/15/17 10:16 AM**
From : **ACME Information Technology Services**
To: **Demo Controller Org (Demo Controller)**
Subject: **Network Malware Warning**

ACME Information Technology Services

RE: Network Malware Incident

Please be advised we are experiencing a significant issue with our internal network. All indications suggest we actually have several computers (at least a dozen) infected with a new and complex ransomware variant. The files on these machines are now encrypted.

We have disconnected all other computers from the network, however our initial investigation indicates the malware has propagated through several enterprise workgroup SANs, impacting all connected resources. We have our System Administrator initiating backup protocols now and should know very soon how long this will take and if there will be any significant data loss.

Also, just in case you're considering paying, the current Bitcoin exchange rate is about $1015.00 US per bitcoin. Each infected machine will require separate payment.

We will keep you posted.

Manager, ACME IT Services

Information Pane

Leadership Team Meeting NEW
Recovery| Analysis of Alternatives

Leadership Team Meeting NEW
Recovery| Potential Options

Company Profile NEW
ACME

Threat Overview NEW
Ransomware
CIP-Ex_Threat Overview

Threat Actor Profile NEW
Threat Actor Profile
CIP-Ex_Threat Actor Profile

Your Desktop Display NEW

Action Pane

QUESTIONS 11 | TIMELINE | ROSTER | QUESTION DASHBOA

0830 Questions
All Questions

Your current situational awareness - Demo Controller Question

At this juncture in the scenario, do you recognize any threat? Select from the following:

(Choose up to 3)
- ☐ So far, nothing out of the ordinary
- ☐ A ransomware extortion attempt
- ☐ A normal level of technical network issues

Possible interrelationship - Demo Controller Question

At this point, are the events you are aware of inter-related?

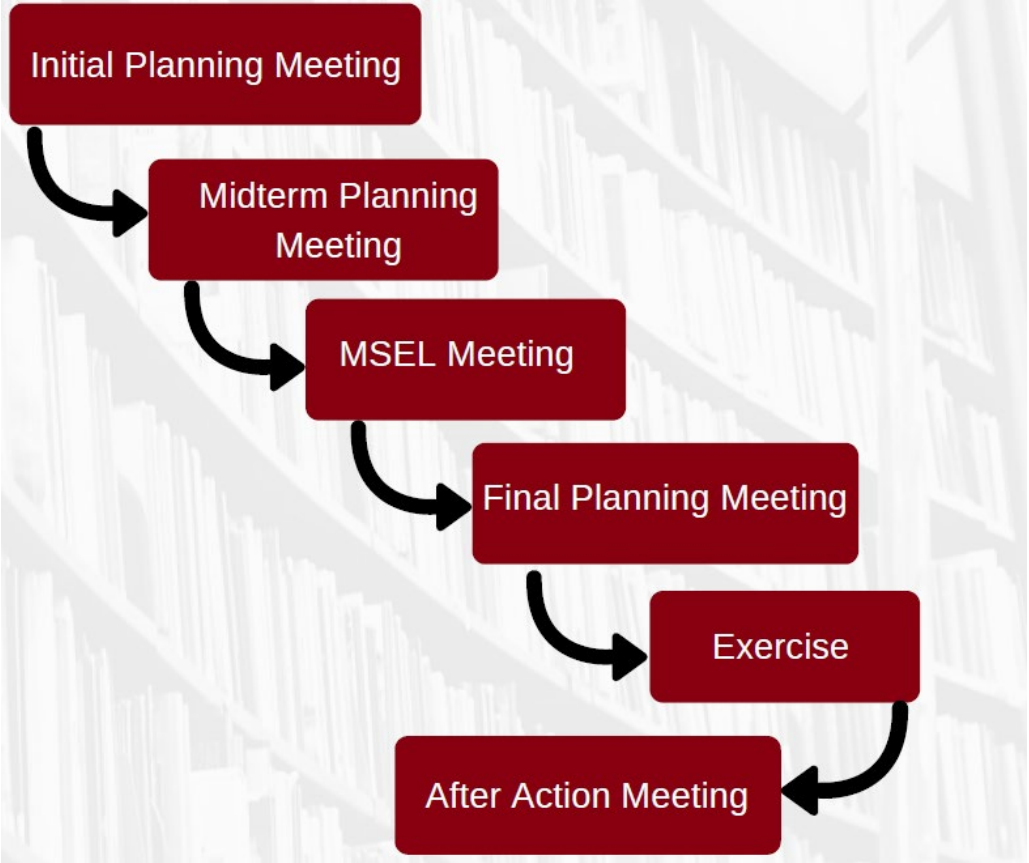
(Choose one)
- ☐ Yes
- ☐ No

SUBMIT

HSEEP/NUARI Planning Process

NUARI provides full exercise planning, design, management, and execution.

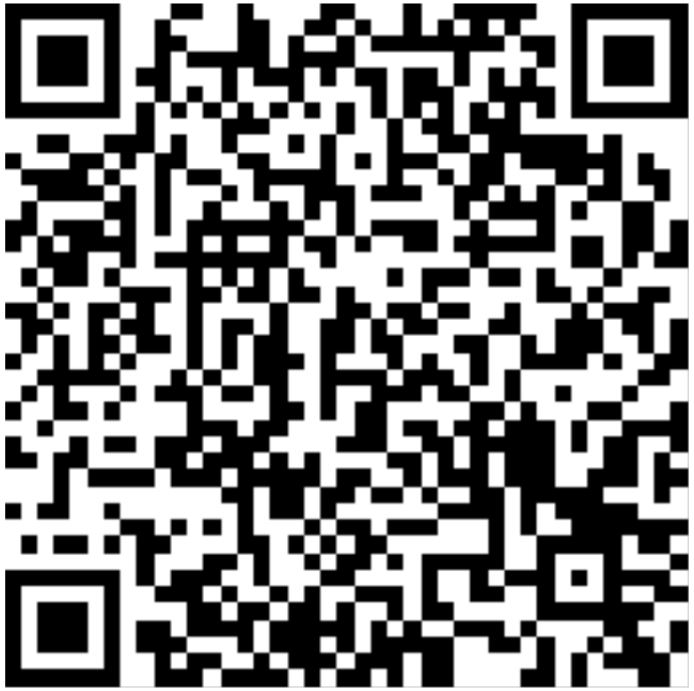
- Exercise planning and project management from kickoff to after-action reporting
- Subject matter expertise and guidance on current and emerging cybersecurity threats
- Scenario, MSEL, and Roster Construction
- Full after-action report including executive summary and raw data reports
- Live executive briefing (virtual or in-person)
- Recommendations for immediate action and identification of areas of improvement



EXAMPLE EXERCISE GOALS

- Practice crisis communications and cross-organization information sharing
- Explore various authorities and responsibilities around a cyber event that spans IT/OT network (e.g. Ransomware affecting SCADA)
- Integrating cyber response with physical response.
- Understand the complexities of dealing with a moderately capable threat actor (e.g. local hacktivist group).
- Local awareness of cyber-physical events in large organizations.

Your feedback is very important to us. Please provide your feedback using the link or QR Code below or the link below:



https://www.surveymonkey.com/r/N9XCL7P

Thank You!

Questions/Discussion

Norwich University Applied Research Institutes

decide® PLATFORM