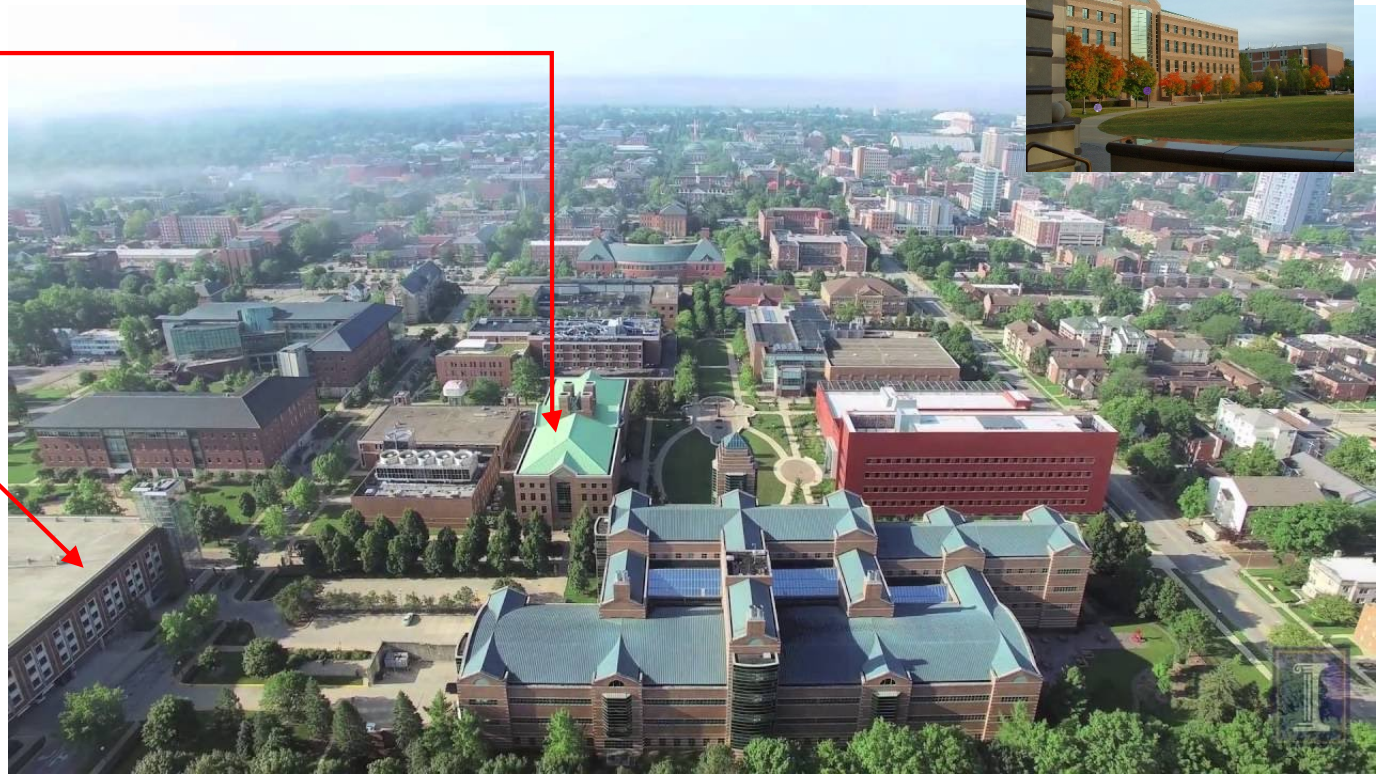
Welcome to Campus



ReCIPE Coalition

The ReCIPE Coalition joins academia, industry and government for the cybersecurity management and defense of critical infrastructure.

The coalition forges a collaborative mechanism through educational content and practical impact to solve pressing regional industrial and governmental cybersecurity issues.

The ReCIPE Coalition will be convening a virtual meeting for coalition members this fall to provide updates and discuss future strategic direction.

ReCIPE Partnership

The University of Illinois, through its Information Trust Institute, in partnership with Iowa State University, is excited to host you this week as you participate in this cyber exercise.

We hope you have a productive two-day exercise, and we welcome feedback so we may continue to design, re-design and create experiences that challenge participants to continuously strengthen their security postures in the face of relentless opposition and increased sophistication.

Event Safety Considerations

Safety and Site Evacuation

In case of an event that requires that we evacuate this building - there are three exit doors on the south side of this building – please exit via the nearest door and move to the Beckman Institute parking lot across the street west of this building.

Lab Environment (David Emmerich)

When in the lab portion of the exercise please be mindful that this exercise will make use of simulated electric grid equipment that contains a live charge, so please act accordingly.

Herman M. Dieckamp Endowed Chair in Engineering
Director, Information Trust Institute

David M. Nicol | Information Trust Institute

dmnicol@illinois.edu

DIRECTOR

BRIEF BIO

Prof Nicol's research include risk assessment of networks and software and scalable virtualized testbeds, research which has led to the founding of startup company Network Perception, and election as Fellow of the IEEE and Fellow of the ACM. He is the inaugural recipient of the ACM SIGSIM Outstanding Contributions award, and co-author of the widely used undergraduate textbook "Discrete-Event Systems Simulation". He holds two patents in cyber-security assessment technologies.

RESEARCH INTERESTS

- Cyber-security of critical infrastructures
- Modeling and analysis of system level security
- Risk-assessment of cyber-threats to critical infrastructures
- Scalable virtualized testbeds
- High performance computing

RELEVANT SKILLS AND COMPETENCIES

Prof David M. Nicol is a member of the Department of Electrical and Computer Engineering. He also serves as the Director of the Information Trust Institute, and the Director of the Advanced Digital Sciences Center (Singapore). He is Principal Investigator for two national centers for infrastructure resilience: the DHS-funded Critical Infrastructure Resilience Institute (ciri.illinois.edu), and the DoE funded Cyber Resilient Energy Delivery Consortium (cred-c.org).

FUTURE WORK INTERESTS

- Virtualized environments for training/workforce development in ICS security
- System-level vulnerability modeling and risk assessment
- Resilient network infrastructure

CORE SKILLS

- Innovation
- Technology
- Modeling and Simulation
- Team Leadership

RECENT and PENDING PROJECTS

- **DOE Cyber Resilient Energy Delivery Consortium**
- **DHS Critical Infrastructure Resilience Institute**
- **Trustworthy and Secure Cyber Plexus**
- **SDN Resilience to Link Failure**
- **Center for Infrastructure Trustworthiness in Energy Systems**
- **Resilient Hybrid PKI**

Doug Jacobson & Manimaran Govindarasu

Doug Jacobson

Principal Investigator
Iowa State University

https://www.ece.iastate.edu/ece-directory/profile/dougj/

Manimaran Govindarasu

Co-Principal Investigator
Iowa State University

https://www.ece.iastate.edu/ece-directory/profile/gmani

RECIPE COALITION

Information Trust Institute - Team Members Supporting Today's Exercise

Matthew Luallen is the Lead Research Scientist for Education Translation where he coordinates a variety of research projects targeting secure critical infrastructure as well as the creation of related educational material.

Dominic Saebeler is ITI's Senior Associate Director responsible for Strategic Planning, Senior Administrative Functions, and Professional Education Projects, and External & Internal Research and Business Development and Industry Stakeholder Engagements.

Casey W. O'Brien is the Associate Director for Cyber Defense Education and Training at ITI where he focuses on various projects related to IT security, education, workforce development and content development and translation.

David Emmerich is a Principal Cyber Physical Range Architect who oversees ITI Lab related activities and numerous associated projects.

Matthew Needham is a Research Systems Administrator who supports the ITI Lab and various security research projects.

Logan Marlow is a Research Programmer responsible for a variety of development projects

Photos & Videos

Capturing the Activities of this Week

Photos & Short Videos

You were asked to sign a photo release prior to arriving or when you signed in. If you do not wish to be in the background of any pictures or videos, please inform us this morning as we may be taking a few pictures and making a few short videos about the exercise.

Any pictures of you will be primarily from back, side or reasonably distant.

Registration & Logistics

Brittney McIntire

Jeni Summers

Dawn Cheek-Wooten

You should have visited one of us to sign in and pick up your badge and Team Assignment

Agenda

Cyber United: Alpha 2.0- Resilient Electric Infrastructure Training (C.U.R.E.I.T) Agenda	
DAY 1 – THURSDAY, APRIL 18, 2024	
Time	**Event Interval Sessions**
9:00 am – 9:30 am	Breakfast provided on site / CSL Studio Kitchen
9:30 am – 10:30 am	Program Start - Exercise Orientation (Room 1232) / Breakfast continues for late arrivals
10:30 am – 11:00 am	All Teams – Breakout Session – Meet and Strategy Session
11:00 am – 12:00 pm	Team Rotation #1
12:00 pm – 1:00 pm	Lunch Provided on site (CSL Studio Kitchen)
1:00 pm – 2:00 pm	Team Rotation #2
2:00 pm – 3:00 pm	Team Rotation #3
3:00 pm – 4:00 pm	Team Rotation #4
4:00 pm – 5:00 pm	Team Rotation #5
5:00 pm – 6:00 pm	Break / Team Rotation #6
6:00 pm	Dinner Provided on site (NCSA Lobby – across the street at 1206 W. Clark)
DAY 2 – FRIDAY, APRIL 19, 2024	
Time	**Event Interval Sessions**
7:30 am – 8:00 am	Breakfast Provided (CSL Studio Kitchen)
8:00 am – 9:00 am	Team Rotation #7
9:00 am – 10:00 am	Team Rotation #8
10:00 am – 11:00 am	Break / Team Rotation #9
11:00 am – 12:00 pm	Team Rotation #10
12:00 pm – 1:00 pm	Lunch Provided on Site (CSL Studio Kitchen)
1:00 pm – 2:00 pm	Team Rotation #11
2:00 pm – 2:30 pm	Exercise Conclusion & Wrap Up Session (Room 1232)
On-Site Location: CSL Studio: 1206 West Clark Street, Urbana, Illinois	

Goals: Provoke thoughts that lead to actions that make your organization more resilient, thereby improving community security

- We will plan to wrap up Hot wash at 45 min.
- Breaks are scheduled to follow hotwash
- Each sessions starts promptly on the hour.

/imagine: C.U.R.E.I.T. goals

C.U.R.E.I.T. exercise

C.U.R.E.I.T exercise effectiveness will be evaluated through a combination of self-assessment, peer assessment, observation, and feedback from participants. Evaluation results will be used to identify areas for improvement and to inform future training programs.

April 3, 2024	**3:00 am – 4:00 pm CST**	**Topic: Incident Response Planning**	**Online Training / Recorded**
April 10, 2024	**2:00 am – 3:00 pm CST**	**Topic: Asset Management**	**Online Training / Recorded**
April 18, 2024	**9:30 am – 6:00 pm CST**	**Exercise On-Site – Day One**	**In Person Only**
April 19, 2024	**8:00 am – 2:30 pm CST**	**Exercise On-Site – Day Two**	**In Person Only**

Educational Content

- This content is educational and in no way conveys a direct recommendation for your systems.
- You, and the **people within organization** need to perform risk management on anything conveyed within this session.
- Considering the aforementioned; there is some great content we will discuss for all backgrounds
  - Firehose is engaged, content will be made available afterwards

RECIPE COALITION

Simple Principles

- Assume eavesdropping, asset theft or loss, and contested territory
- Know your system's hardware, software configuration and communications patterns and alarm upon attempted to actual changes
- Have established procedures and protocols with authority
- Build with moats (controls)
  - Understand how the moat (control) works
  - Define trusted methods to cross the moat
  - Strongly authenticate (trust) any attempted moat crossing (cyber, physical)
  - Establish fake (honeypot) systems and monitor / react
- Use established resources, like **PEOPLE with Tooling**
  - **Tooling with data to analyze (Backups, Span/Tap, Logs)**

Rotations

Structure of each rotation

1. Training: The training will provide hands-on how to steps of adversarial tactics that may be used during exercise stage.
2. Exercise: The exercise will introduce a situation that will cause the trained skills to be used in an escape room style to leverage all capabilities and further enhance team communication.
3. Hot Wash: The hot wash will cover the success, failures and lessons learned during the exercise.

Sessions

Three Active Sessions:

- Session 1: Asset Inventory Management
- Session 2: Initial Threat Detection
- Session 3: Finding Solutions

Additional Sessions:

- General Session A: SBOM
- General Session B: Cyber Awareness

RECIPE COALITION

Training

Session 1: Asset Inventory Management

- Investigate the MITRE ATT&CK framework
- Review pathfinder to perform discovery operations
- Generative prompts that may help you during the exercise

/imagine: cyber asset inventory management

RECIPE COALITION

Exercise

Session 1: Asset Inventory Management

Perform physical asset discovery and compare with documentation

Use Wireshark on tap points to visualize environment (span and rspan)

Gain initial access to systems to perform active and passive host analysis (nmap, powershell, system tools, event viewer)

/imagine: cyber asset inventory management

RECIPE COALITION

Hotwash / Break

Session 1: Asset Inventory Management

What did you find?

How did you find it?

What else could you use to be more efficient?

What real world challenges occur with Asset Inventory Management?

What questions do you want to ask, and tasks do you want to perform during the next sessions?

/imagine: cyber asset inventory management

RECIPE COALITION

Training

Session 2: Initial Threat Detection

- Investigate threat actor operations
- Review categorized adversarial abilities
- Generative prompts that may help you during the exercise

/imagine: initial threat detection

RECIPE COALITION

Exercise

Session 2: Initial Threat Detection

- Continue performing physical asset discovery and compare with documentation
- Continue to use Wireshark on tap points to visualize environment (span and rspan) while review on system activity (netstat, task manager)
- Use generative prompts to help you perform detection operations

/imagine: initial threat detection

RECIPE COALITION

Hotwash / Break

Session 2: Initial Threat Detection

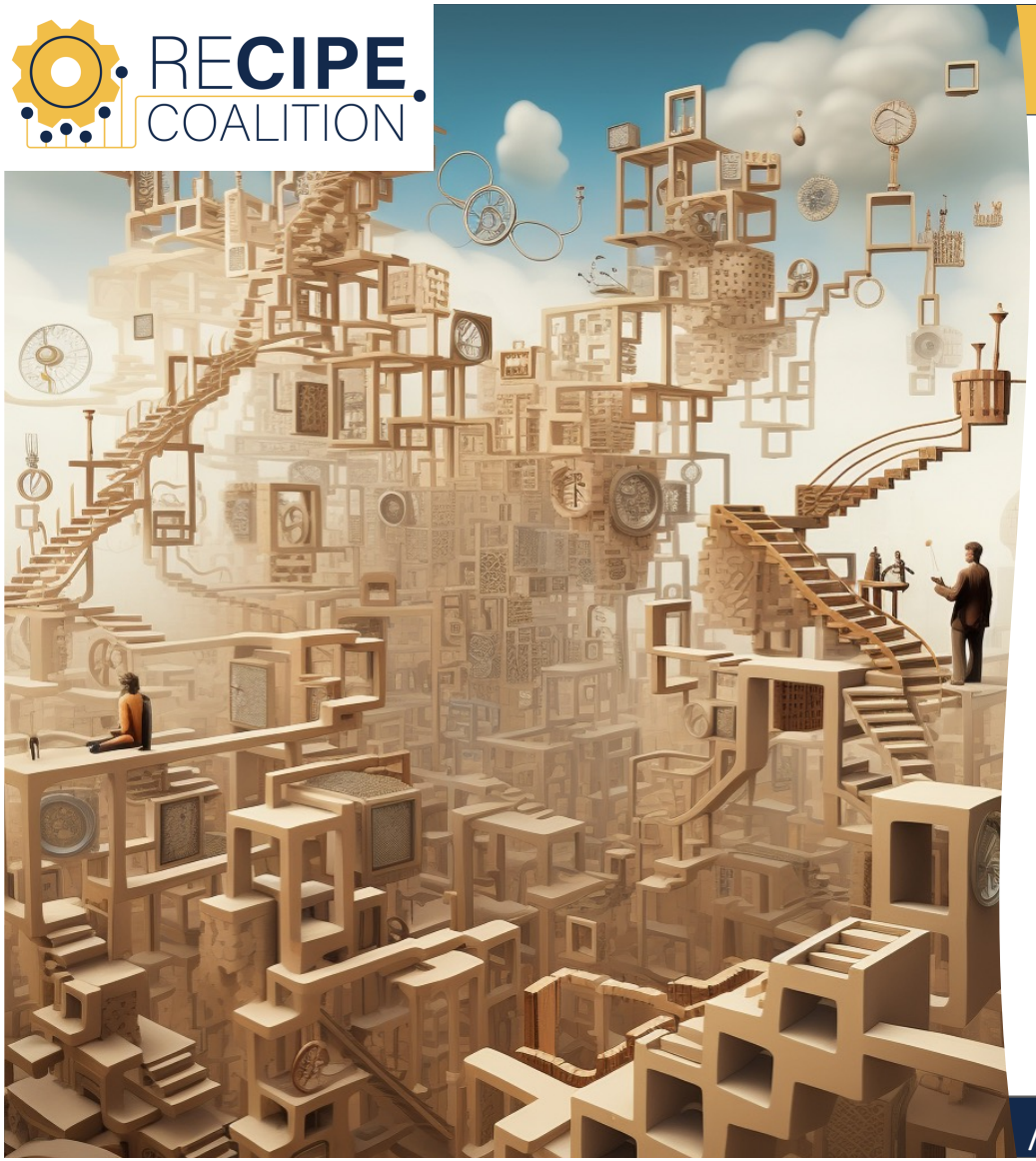
What adversarial abilities are you concerned about?

What real world challenges occur with detecting threats?

What questions do you want to ask, and tasks do you want to perform during the next sessions?

/imagine: initial threat detection

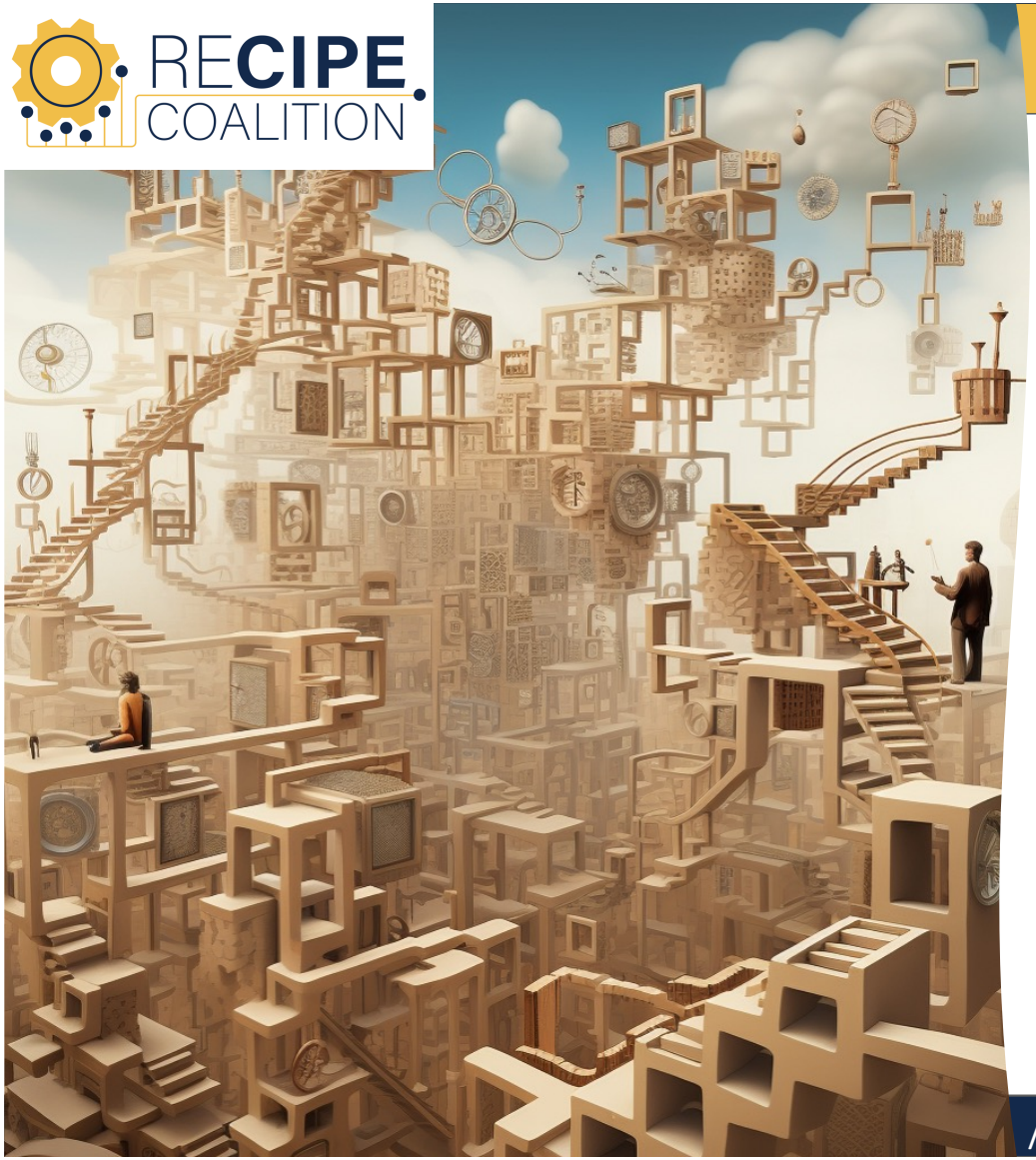
RECIPE COALITION



Session 3: Finding Solutions

- Threat actor operation results
- Adversarial capabilities of “living off of the land”
- Generative prompts that may help you during the exercise

RECIPE COALITION



Exercise

Session 3: Finding Solutions

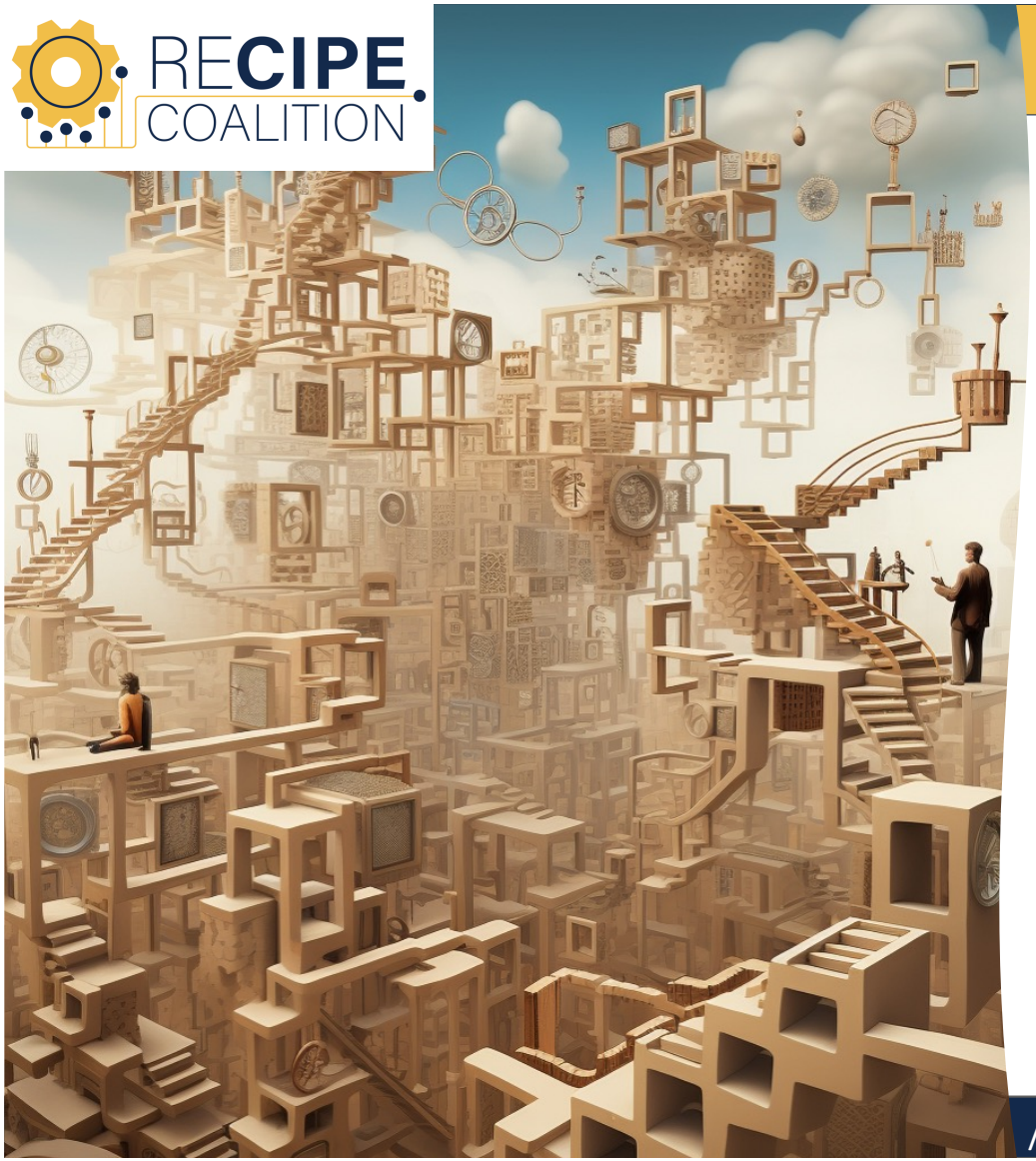
What are some of the best options available to you to continue to operate while compromised?

What systems have been impacted and how can you confirm their validity?

Use generative prompts to help you perform detection operations

/imagine: finding solutions

RECIPE COALITION



Hotwash / Break

Session 3: Finding Solutions

What kind of threat actor activity did you identify?

Does it seem realistic?

How will you defend against this type of threat?

What questions do you want to ask, and tasks do you want to perform during the next sessions?

/imagine: finding solutions

RECIPE COALITION

General Session A: SBOM

- Vendor solution examples for Software Bills of Material (SBOM)
- What is the attack surface and what are the best methods to secure it?
- What else would you like to know about the vendor's solution?

RECIPE COALITION

General Session B: Cyber Awareness

- Recent CISA announcements
- Living off the Land
- Helpful frameworks

Thanks!

So where do I go now ?

Schedules are Posted in Each Room

- 1232 – We are in room 1232
- 1221 – The small conference room west down at the end of the hall
- 1236 – The exercise Lab directly across the hall

We will start the Sessions at 11:00 am sharp

Observers can select their first Session if they are not following one of the Teams. Please join the SBOM session at 1 pm Day two if you are not part of one of the teams.

Exercise Wrap Up & Conclusion

Day Two Wrap-Up: 2 – 2:30 pm

- Lessons learned
- Feedback
- Interesting comments
- Letter of Support Request
- Note Board Comments/Highlights
- Follow-up discussions
- Event Photos
- Next Steps
- ReCIPE Members Update Session later this year

Commitment Letters from Participating Utilities

University of Illinois – DOE FOA Proposal Submission

We are planning to submit a proposal to DOE in early June.

We will be asking for 3 years of funding starting in 2025.

Funding will support our time to design, host and deliver in person and online training and exercises that will be based off this CUREIT exercise theme.

Ask: we simply need you to send us a letter indicating support – so you are permitted to receive the benefits of future exercises and training like this one. We will send you the letter content – you simply need to place it on your letterhead, sign and return then you are eligible.