2024 InCommon Cybersecurity Exercise Information

1.1. Current Status: 2024 Planning Activities Initiated

RESOURCES FOR PARTICIPANTS

The following links are resources for participants during the exercise. They have been sent to each organization's exercise POC, but are included here for convenience.

- REFEDS Metadata Extraction Tool (MET)
  Primary easy tool when given an entity ID returns the organization information to include security contacts. Note that the security contacts are tagged as 'other'.
- InCommon member list
  Tool when given an organization's name, returns the federation metadata information to include security contacts.

EXERCISE CONCEPT AND EVENTS

Welcome to the InCommon Cybersecurity Exercise information page. Calls for participation will go out mid August out seeking interested organizations.

The following information further explains the exercise concept.

Overview

We will ask your designated exercise Point of Contact (POC) to act as a trusted agent for our exercise coordination cell during the exercise, which will include a training and orientation session prior to the exercise. Our success depends on each organization's POCs being active participants to help us run the scenario over a distributed group of participating organizations. We will coordinate with your exercise POCs to help you determine whom you want to designate within your organizations as exercise participants.

The primary purpose of this event is to practice using the Sirtfi framework to coordinate cybersecurity incident response between affected organizations. There will be no real-world technical events or actions on the network; all breaches, security investigations, log files, etc., will be simulated in a narrative. The SEPWG will publish guidance to all exercise POCs and exercise participants on how to mark any communications (e.g., emails, slack messages, etc) as exercise communications so they are not mistaken as real-world events.

Exercise participants will only be performing four "real-world" tasks as they discuss the narrated scenario and interact with the exercise control cell (via the exercise POCs you've designated as our trusted agents):

1. Recognize when the scenario indicates when the activity affects other external federated organizations, which prompts the need to use the Sirtfi framework.
2. When given a username/organization, finding that user's Security Contact, as required to be published by the Sirtfi framework.
3. Establishing communications with an external organization using the Sirtfi Security Contact.
4. Receiving and responding to requests to the Security Contact, identifying those requests as Sirtfi requests, and partnering as appropriate depending on the narrated scenario event.

All other tasks will be simulated through tabletop narration.

Schedule of Events

We plan three key events: two preparatory events culminating in the distributed tabletop scenario itself.

1. (In Planning) Communications Test: *Date TBD ~ Oct*

This event will involve minimal time from your organization. Towards the beginning of the week, we plan to email a test message to your published Sirtfi Security Point of Contact, and ask for acknowledged response.

Once we receive acknowledgement, we will notify your Exercise POC (Trusted Agent) that response was received. If we get to the latter part of the week and don't get a response, we'll reach out to your exercise POC.

2. (In Planning) Exercise Orientation for Exercise POCs: *1 Hour Zoom Event, Multiple sessions offered, Dates TBD ~Oct*

In October, our working group will host a one to two hour sessions over zoom for all exercise POCs. Each POC need only attend one session; multiples are offered to accommodate people's schedules.

This session will provide an orientation to how the exercise will run, and what we'll need from the Exercise POCs during the exercise to make this event successful. We'll also provide the vision on what your exercise participants will be expected to do and how the Exercise POCs will work as a liaison between our SEPWG Exercise Control Cell and the exercise participants themselves. During this event, the SEPWG will walk through a piece of a scenario we practiced last May, to illustrate how the Exercise Control Cell (ECC), the exercise POCs and the exercise Participants work together to advance the scenario. This orientation will ask for one to two hours of your exercise POC's time, and there may be minimal time required on their end to confirm participating members within your organization. At a minimum, we will ask your exercise POC arrange to have a person who receives and can respond to emails sent to your Sirtfi Security Contact.

3. (In Planning) Distributed Tabletop Exercise: *November 18 - November 22*

In November, we plan to run a scenario involving multiple organizations over the course of the week. Your organization will be scripted into a scenario along with 3 to 5 other participating organizations.

On Monday, there will be a kickoff presentation open to all participants. The actual scenario will take place Tuesday through Thursday. On Friday there will be a zoom room open for all exercise POCs to relay lessons learned, positives, and areas for improvement. This session will also be open to any participant who wishes to attend.

We do not expect organizations to have participants dedicated full time throughout this event. Likely, this will impact your participants from between one and two hours during the event, but not necessarily all at once. Some organizations may be finished on the first day with their part of the exercise. Others might not see an input until the second or third day. We've budgeted three days to allow for a natural communication flow and to account for delayed responses due to time zone differences. The Exercise Control Cell (ECC) will not be operating 24x7 during this exercise, but will be responsive during the normal working day (in the US). More specific times will be detailed the closer we get to the event.