SIRTFI Exercise Planning Working Group End of 2022 After Action Report

Repository ID: TI.174.1
Persistent URL: http://doi.org/10.26869/TI.174.1
Publication Date: December 15, 2022
Author: Kyle Lewis, SIRTFI Exercise Planning Working Group (SEPWG) Chair
Sponsor: InCommon Community Trust and Assurance Board

To: InCommon's Community Trust and Advisory Board (CTAB)

From: Sirtfi Exercise Planning Working Group (SEPWG) Chair

Subject: End of 2022 After Action Report

Summary

In 2022, the SEPWG planned and conducted InCommon's first community Cybersecurity Cooperation Exercise, focusing on the Sirtfi framework. Ten organizations from the InCommon federation volunteered to participate. In November, the SEPWG conducted the exercise with the participating organizations and collected feedback, presenting the results at the 2022 TechEX/CAMP Week. Feedback was positive, and the event was a successful demonstration that we can do these kinds of events in the federation. The bottom line recommendation is to re-charter the SEPWG for 2023 to evolve the learning activities and continue to give member organizations the chance to practice using the Sirtfi framework.

Details

The SEPWG was formed to provide federation member organizations' security teams opportunities to practice using the Sirtfi framework to facilitate communication and coordination during cybersecurity incidents.

The SEPWG adopted a three phased approach, plus a "Phase 0" preparatory step for the working group.

During Phase 0, the SEPWG walked through a basic script to practice how to run an exercise and get an understanding of how participants would play in the exercise. Upon completion of Phase 0, SEPWG requested InCommon send a call for interest. 17 organizations responded. Two were removed due to incomplete forms, no federation membership, and unresponsiveness to requests for clarification. Five more were eventually removed due to unresponsive points of contact (POCs).

Ten organizations volunteered, were engaged, and participated in Phases 1 through 3:

1. CA Poly State University-San Luis Obispo
2. CILogon
3. Elsevier
4. Laser Interferometer Gravitational-Wave Observatory (LIGO)
5. National Institute of Allergy and Infectious Diseases (NIAID) International Team
6. National Institutes of Health (NIH)
7. North Dakota State University (NDSU)
8. Online Computer Library Center Inc (OCLC)
9. Rice University
10. University of Illinois (had to drop during the exercise due to real-world events)

For Phase 1, the SEPWG conducted a communications test. The SEPWG used the POC's submitted entity IDs to look up each organization's Security Contact. Phase 1 consisted of the SEPWG sending emails to each Security Contact requesting acknowledgement. For those that did not respond, the SEPWG followed up with the respective organization's POC. Most organizations responded within a few hours. One organization discovered they had the incorrect Security Contact email published to the federation, and took action to fix. Another organization's Security Contact email feeds a ticketing system, and they discovered their internal ticketing notifications weren't working. That organization also took action to fix. Both organizations had things fixed for the exercise.

Phase 2 consisted of training all the organization's exercise POCs on how the exercise would be orchestrated, and their respective roles.

Phase 3 consisted of the actual exercise. It was a 3 day scripted event starting on Tuesday and ending on Thursday. It was book-ended by a kickoff session the Monday before the script started, and a wrapup session on Friday.

All files, to include the exercise scripts, training, kickoff and wrapup presentations, outbrief at TechEX, and documentation on the phased methodology is recorded in the SEPWG online folder, and available for future planning teams.

Observation by the SEPWG through the course of the year is that finding a Security Contact in the midst of an event cannot be assumed to be a known process in the midst of a security incident. Continual practice helps spread knowledge of how to find Security Contacts, and also fosters a "federation mindedness" in security response teams who may be otherwise unfamiliar with federation activities in their day to day operational routine.

Specific feedback from the SEPWG ECC and exercise participants was recorded in the wrapup session slides, and included below in Attachments 1 and 2. All organizations expressed the need to practice more and want to see the SEPWG work continue in 2023. Some participants expressed willingness to volunteer for next year's working group.

Takeaways

People need practice looking up security contacts. People need practice communicating externally during incidents. Our community cannot be assumed to be prepared for real-world cross-organization cybersecurity incidents without making coordinating actions part of routine practice. The organizations who participated validated an appetite for more events like this.

Recommendations

Recommend CTAB send out another call for volunteers for an SEPWG kickoff in Jan 2023, and re-charter the group. Call for volunteers would also be forwarded directly to last year's exercise POCs from the volunteering organizations to get the word to this year's players who expressed interest in helping next year.

Respectfully,
Kyle Lewis
SEPWG 2022 Chair

Attachment 1: ECC feedback from SEPWG perspective

- Ask organizations' exercise POCs what timezones their participants are in (not always the same) so we can make sure more westerly zones get written in as … not the first.
- Scripting at a pace of two organizations per day seems right
- Need to improve narrative richness of exercise injects (e.g., timestamps for simulated activity)
- Ask orgs for primary and alternate POCs
- Communicate with POCs the need to make their participants aware and attend the kickoff orientation (some time lost due to some players not knowing there was an exercise)
- Give time/set environment for more back and forth participation between participants
- Internal to ECC: how to involve more ECC members given the distributed environment vs 1 person running script per exercise team (in our case 1 person running both scripts due to real world events)
- ECC did not see all traffic between organizations (sometimes, were informed by POCs that message happened, but didn't get actual message; hard to get a feel for how many used TLP markings)
- If organization provides multiple entities (e.g., 1 SP and 1 IdP), pick the one that fits the script rather than impact the organization's real-world responsibilities twice in the same week vs once for the others
- Next year the scenario needs to test TLP knowledge

Attachment 2: Participant feedback during wrapup session

- Cal Poly: agrees letting participant team know in advance; took advantage of opportunity to review documentation with SOC; communication incoming was not TLP marked; REFEDS MET does not include security tag (bottom line: worthwhile; prompted internal impetus to do internal TTXs with lessons learned from here)

- OCLC: appreciated the chance to participate; wants more TLP injects/objectives; our emails don't come from our security email (it's a distro list); more emphasis on checking message authenticity; not all organizations will send from the security contact; add need to request information across organizational boundaries in script (bottom line: overall good exercise)
- NDSU: pri and alt POCs! Our team got ahead in shaping the narrative before the RFI went to the ECC and got the actual information; include timestamps; what about including IPv6? (overall: very good exercise)
- CILogon: definitely worthwhile; agree with pros and cons of distributed; interested in an in-person TTX/workshop at something like a TechEX); give feedback to InCommon and REFEDS on difficulty of finding security contacts
- NIAID IBRSP: overall good; we've done them internally in the past, but having real external players helped break an insular mindset of not being used to reach out externally; agree to wanting more TLP practice; also: we need to do more internally; found the process uncomfortable because it was not easy; what will help is practicing more
- Rice University: participant team not sure it was worthwhile; waited until day 3 for a very simple inject; didn't have to consult response playbook; looking for more in-depth "rich" inputs, with more urgency; POC thinks the exercise was good and has been encouraging TTXs; glad to see TTXs are started; interested in CILogon's suggestion of an in-person TTX; also, mini-TTXs: overall wants to see this practice continue and mature