Exercise Documentation - Version 1

Organised by:

iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design

Ministry of Defence, Singapore

Funded by:

Ministry of Defence, Singapore

National Research Foundation, Singapore

Supported by:

Cyber Security Agency, Singapore

Duration:

6 to 17 Sep 2021

Exercise Team:

Exercise oversight & management

Reuben Chng
Mark Goh
Lim Keng Yan

Technical Support

Mavis Ang
Andrew Tay

Sponsoring Partners

Fortinet
Gigamon
Tegasus

Exercise Platform & Tools

Chow Wong Chong
Ivan Christian
Matthew Cruz
Ivan Lee
Aditya P Mathur
Andres Felipe Murillo Piedrahita
Nicholas Png
Gauthama Raman Mani Iyer Ramani
Athalye Surabhi Sachin
Shao Hong Sze
Siddhant Shrivastava
Bryan Wong

TABLE OF CONTENTS

Version History

Version No.	1
Effective Date	18 June 2021
Revision Date	
Major Revision(s)	

1. Objectives

1.1 CISS2021-OL aims to meet the following key objectives: (a) validate and assess the effectiveness of technologies developed by researchers associated with iTrust; (b) develop capabilities for defending critical infrastructure under emergency situations such as cyber-attacks; and (c) understand composite Tactics, Techniques and Procedures (TTPs) for enhanced Operation Security.

1.2 In addition, CISS2021-OL will enable Red Team members to understand approaches for compromising critical infrastructure and hence what protection mechanisms are necessary.

2. History & Modality

2.1 The exercise began in 2015 under the event named Secure Cyber-Physical (SCy-Phy) Systems Week. In 2019 it was renamed as Critical Infrastructure Security Showdown (CISS) to better reflect its purpose and domain. In 2020, owing to the global pandemic CISS was moved to a **fully online** exercise, where all participants, i.e. Red and Blue Teams, launched and monitored attacks online, respectively, from wherever they are based.

2.2 CISS2021-OL will see the retention of the online platform modality, with the following additions:

a) World Wide Web as entry point
b) Water Distribution (WADI) testbed as additional attack surface
c) 5 hours for Red Teams to launch attacks (instead of 4)
d) Intrusion Detection Systems (IDS) installed
e) Higher score for Red Teams that can avoid IDS detection
f) Higher score for Red Teams that use reflector servers to mask their identity
g) Prize money for Red Teams doubled

2.3 CISS2021-OL is divided into two weeks to meet distinct objectives.

a) Red Team Exercise (6 to 10 Sep): Each Red Team is given 5 hours to launch attacks on the platform and gain points when they meet attack objectives. Blue Teams Vendors are commercial companies

who have installed their products to detect Red Teams' attacks. Red Teams' TTPs are captured during this week. Red Teams and Blue Team Vendors' participation are by invitation only.

b) Blue Team Exercise (13 to 17 Sep): A composite Red Team will be form by various organisations to launch attack on the platform, which will be defended by Blue Teams that comprises Critical Information Infrastructure (CII) operators and regulators ("CII Blue Teams".) Each CII Blue Team is given one slot of 8 hours to respond to the attacks and defend the platform. The five CII Blue Teams' participation are by invitation only.

2.4 There are four classifications of participations in CISS2021-OL: (1) Red Teams, (2) Blue Team Vendors, (3) CII Blue Teams and (4) Observers. The makeup of participants in each category follows:

a) Red Teams (up to 4 members):
   - Up to 10 local and international teams from government organisations, private sector and academia
   - Stage 1 will be organised in July to admit top 10 Red Teams into the Finals (Red Team Exercise from 6 to 10 Sep.)
   - **Anonymity is provided upon request**

b) Blue Team Vendors (no limit on the number of members):
   - One from iTrust, comprising a variety of anomaly detectors
   - Commercial vendors will be invited based on their past performance in similar events and nominations by Singapore Government agencies
   - Academia from centres around the world that have cyber-security as their prime focus and have demonstrated research record in securing critical infrastructure
   - **The anonymity of Blue Teams is, by default, maintained throughout**

c) CII Blue Teams (6 to 10 members):
   - CII operators and regulators

- **The anonymity of Blue Teams is, by default, maintained throughout**

d) Observers: Singapore Government agencies and their invitees. iTrust will execute the event online from where any authorised observer can track the progress - in terms of attacks launched and detected - of the event.

3. Phases in CISS2021-OL

	Date	Details	Involvement
Stage 1	5 – 16 Jul	Stage 1 (3 hours per team) to admit 10 Red Teams to final round	Red Teams
Online Briefing	23 Jul	Rules of engagement, attack objectives (Red Teams) Alert reporting (Blue Teams) Virtual tour of platforms (all) Q&A (all)	Red Teams
	26 Jul		CII Blue Teams
	30 Jul		Blue Team Vendors
Submission of VMDK	30 Jul	Red Teams to submit VMDK containing their attack tools to organisers	Red Teams
Familiarisation	4 – 13 Aug	Testing VPN, RDP, attack tools	Red Teams
Onsite deployment	16 – 20 Aug	Deployment/setup onsite	CII Blue Teams
Onsite deployment	16 – 27 Aug	Deployment, baselining of products	Blue Team Vendors
Familiarisation	23 – 27 Aug	Virtual familiarisation (3 hours per team)	CII Blue Teams
CISS2021 Finals	6 to 10 Sep	Red Team Exercise	Red Team, Blue Team Vendors
	13 to 17 Sep	Blue Team Exercise (closed door)	CII Blue Teams

3.1. Stage 1 [5 to 16 July]

3.1.1. There are 10 Red Team slots in the Red Team Exercise Finals that will be held from 6 to 10 Sep. Stage 1 is organised to admit the 10 Red Teams into the Finals, based on their performance in Stage 1.

3.1.2. Each Red Team is given 3 hours (1000 – 1300 hrs or 1400 – 1700 hrs, GMT+8) to meet a set of attack objectives. The top 10 teams that achieve these objectives in the fastest time will be admitted into the finals. Please use this link to book a slot for Stage 1. **While a team name is encouraged** when making a booking, please inform the organisers (itrust@sutd.edu.sg) after a booking has been made, so we know who has made the booking.

3.2. Online Briefings [23 to 30 July]

All teams will be given:

a) Information on exercise platform including Secure Water Treatment (SWaT), Water Distribution (WADI), World Wide Web, Zycron Cyber City and the various anomaly detection and plant safety technologies
b) An online tour of the SWaT and WADI testbeds and have their questions answered.
c) Access to past data collected from SWaT and WADI, as well as data collected during CISS from 2017 to 2020.
d) Past CISS reports can be assessed here: 2016, 2017, 2019, 2020

3.3. Submission of VMDK [30 July]

3.3.1. To be updated

3.4. Familiarisation by Red Teams [4 to 13 August]

3.4.1. To be updated

3.5. Deployment by CII Blue Teams [16 to 20 August]

3.5.1. To be updated

3.6. Familiarisation by CII Blue Teams [23 to 27 August]

3.6.1. To be updated

3.7. Product deployment & testing by Blue Team Vendors [16 to 27 August]

3.7.1. Blue Team Vendors who need to install hardware in SWaT will be given 2 full days to do so. Please make your bookings using this link. Whenever possible, iTrust will set aside time to supervise the installation by the Blue Team Vendors. Importantly, Blue Team Vendors shall ensure that:

- They supply, deliver and set up their own systems, including but not limited to hardware, servers, accessories and peripheral devices.
- Their installations do not disturb the regular plant operation and interfere with existing iTrust technologies;
- They will make its own arrangements for the data generated by its hardware to be piped to their computers outside of the SWaT and WADI during the exercise;
- Their installations respond as if in a real-time environment;
- Their installations (hardware and software) be completely removed post-exercise and restore SWaT and WADI to their original condition. They shall bear any cost for damages arising from the installation and/or teardown of the upgrades; and
- There shall be no efforts made to prevent, halt or thwart any attacks launched by the Red Teams.

3.7.2. iTrust will not provide any additional hardware / software for installation / setup / GUI display to Blue Team Vendors, should there be any physical equipment to be set up in SWaT.

3.7.3. Blue Team Vendors' systems will be connected to iTrust's TAP switch to receive pcap data from Zycron Cyber City, SWaT and WADI. Ethernet cables will be provided for this purpose. **As Blue Team Vendors will not have physical access to the platform, they will need to set up remote monitoring capabilities to view their systems' GUI off-site over SUTD's WiFi or its own 4G router.**

3.7.4. Details on attack detection and reporting by Blue Team Vendors will be provided at a later date.

3.8. CISS2021-OL Finals

3.8.1. Red Team Exercise (6 to 10 Sep)

The Red Team Exercise Finals will be spread over 10 Red Team Slots from 6 to 10 Sep (Mon – Fri). The duration of each slot is 5 hours and is scheduled from 0900 hrs to 1400 hrs or from 1500 hrs to 2000 hrs (GMT+8) daily, with a one-hour break in between for system reset. The Red Team attack schedule will be announced on the website two weeks before the exercise.

3.8.2. Blue Team Exercise (13 to 17 Sep)

The Blue Team Exercise is a closed-door event and by invitation only. CII Blue Team invitations have been sent out and teams have been formed. Blue Team vendors and academic institutions who are deploying their products in the Red Team Exercise can continue to have their products deployed during this week.

3.8.3. Attack platform

For added realism, all Red Teams must attack SWaT by first entering the network via a simulated World Wide Web. They will then attempt to land in Zycron Cyber City's corporate network to gain access to the testbeds (see Figure 2.) ZCC is a full-fledged virtual organisation comprising of Information Technology (e.g., e-mail server, file server, printer server, CCTV, honeypot and intranet) and Operational Technology (processes similar to those in SWaT). To make these entities "alive," various types of network traffic are also crafted and included in ZCC. As an IT environment, ZCC is not set up with best practices i.e., it is intentionally built with minimum security features and contains vulnerabilities for Red Teams to explore and exploit. Note that there is no internet access within the ZCC.

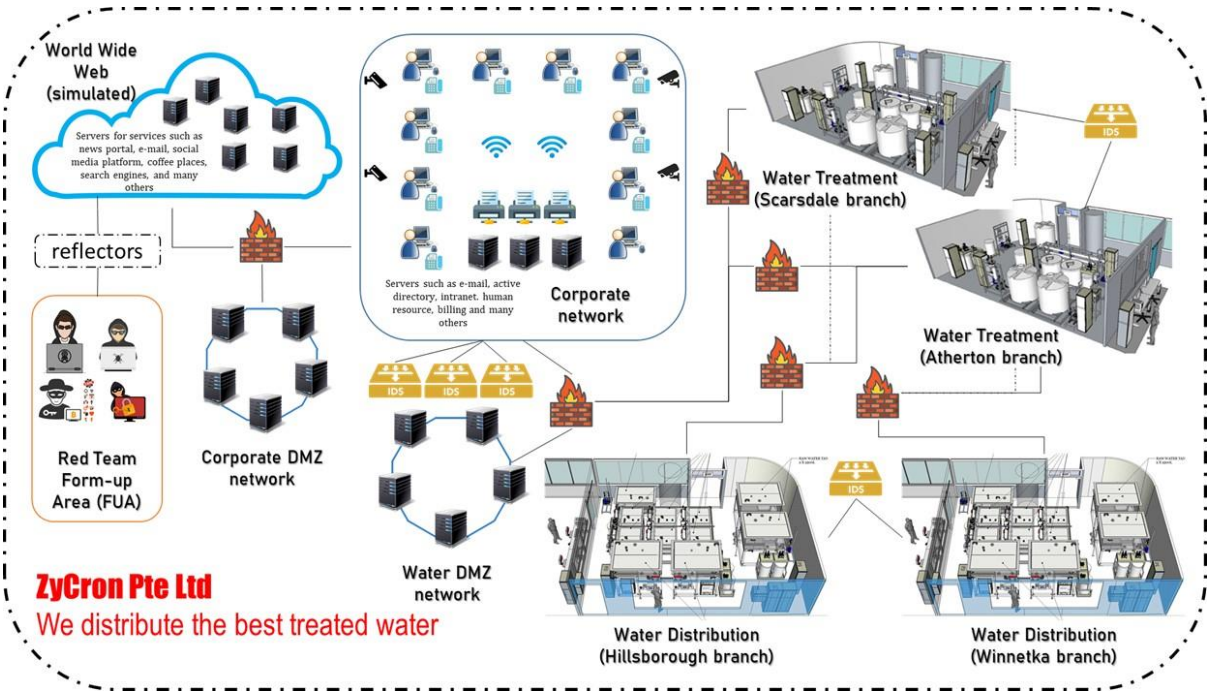

Figure 2: High-level Architecture of CISS2021-OL Attack Platform

3.8.4. Launching attacks

Active teams will design and launch attacks on SWaT for 5 hours. Prior to launching attacks, the active Red Team must do the following throughout its allotted 5-hour slot:

a. Share with iTrust the "live" screen of all team members' computers used during the exercise via an online communication tool (e.g. Zoom)[1];
b. Allow iTrust to record their screens (video and audio); and
c. Inform judges (1) the intention of the attack; (2) the targeted component(s); and (3) the launch procedure.

The duration of an attack will be determined in real time by iTrust's cyber security technology engineers stationed physically at SWaT. Attacks that take a long time, e.g., 30 minutes, to have a noticeable impact on the plant will likely be halted by the judges before the impact is visible.

[1] This is purely for iTrust's post-event analysis and report writing purposes; recordings will not be shared or made public with anyone without written permission by the Red Team

3.8.5. Attack monitoring

Any anomaly resulting from the attack, or otherwise (i.e., a false alarm), and reported by one or more iTrust detectors, will be visible **only to the organisers, observers and judges and not to the Red or Blue Teams.**

3.8.6. Scoring of Red Teams

The performance of Red Teams will be assessed in real-time by a team of judges consisting of cyber security experts and engineers working in the critical infrastructure domain. **Only single attacks, in series, are allowed i.e. an attack can only begin after the previous one has ended/aborted.** All teams that successfully complete the exercise will be given a certificate of participation. Judges will score each team based on criteria such as complexity of the attacks launched and success of the attack in resulting in an anomaly in at least one of the plant state variables. **Top three Red Teams will receive cash prizes of S$4,000, S$2,000 and S$1,000 respectively.** The total score, *S*, for each attack launched is computed based on five factors:

$$Total\ score,\ S = \sum_{i=1}^{n} A_n E_n T_n - I + B$$

where:

- **A = Attack Score**
  - Achieving different attack objectives will be rewarded with 100 – 400 points, depending on their difficulty; a separate document will be sent to Red Teams
- **E = Entry point factor**
  - Red Teams are rewarded if they use a reflector server to mask their identities
  - E = 1.3 if a reflector server is used; else, 1.0
- **T = Teleport factor**
  - If attempts to enter into SWaT are unsuccessful after 30 mins (request to extend to up to 60 will be considered), the team may request to be teleported to attack SWaT or the digital twin directly
  - T = 0.5 if teleport required; else, 1.0

- **I = IDS penalty**
  - IDS is installed in ZCC and the SWaT testbed. If an attack launched by the Red Team is detected within a 30-min window, 50 points will be deducted
  - Maximum deduction over 5 hours: 500 points
- **B = Bonus points for disarming IDS**
  - The disarming itself must not raise any alarms within the IDS
  - Each successful disarmament earns 200 points

3.8.7. Attack detection and reporting of alerts by Blue Teams

It is important for Blue Teams to note that CISS2021-OL is being conducted to simulate attacks on a live city-scale plant. Hence, it is assumed that the security systems deployed by each Blue Team are operational throughout the exercise except when SWaT and WADI are not running or being reset.

3.8.7.1. Attack detection

Throughout the event the Blue Teams will monitor their systems remotely (more details will be provided). Post-event, Blue Teams will be given selected pcap and OT data captured for analysis. To recap para 3.7.1, **there shall be no effort made by the Blue Teams to prevent, halt or thwart any attacks launched by the red teams.**

3.8.7.2. Reporting of alerts

The above assumption implies that any alert generated by the security system deployed by a Blue Team must be reported ***immediately*** to the plant operator ***automatically, not manually***. While each Blue Team will be provided all event data, e.g., pcap files and Historian data, at the end of the event, they are not expected to conduct an analysis of an alert generated ***during*** the event. ***Again, each alert must be reported immediately as if it is occurring in a live plant and being reported to the plant operator.***

Reporting of alerts to iTrust by Blue Teams must be done so in one of the following two ways:

a) PEPPR-PV: this would require the Blue Team to work with iTrust's developer to integrate with it, so that its detections/alerts can be sent to PEPPR-PV for automatic logging and visual alerts; or
b) Alert logger: a simple password-protected interface to manually log a time-stamped alert each time the Blue Team detects an attack.

4. Acceptance of Terms & Conditions

Participants who register for this exercise are deemed to have read and accepted all the terms and conditions set out in this document. iTrust reserves the right to change these terms and conditions at any time up until the exercise, without prior notice.

<End of document>