The Fourth International

CISS

Critical Infrastructure Security Showdown - Online 2020

Event Plan V5.0

Sponsors:

National Research Foundation, Singapore

Ministry of Defence, Singapore

Duration:

July 27 - Aug 7, 2020

Event Team:

Event oversight and management

Mark Goh

Beebi Siti Salimah Binte Liyakkathali

Teo Jia Hao, Ian

Technical support

Ivan Lee

Muhammad Syuqri Bin Johanna

Siddhant Shrivastava

Student volunteers

Francisco Caetano Dos Remedios Furtado [MINDEF Red Team support]

Tools

Aditya P Mathur

Gauthama Raman Mani Iyer Ramani

Athalye Surabhi Sachin

Ivan Lee

Siddhant Shrivastava

TABLE OF CONTENTS

Version History

Version No.	5.0
Effective Date	13 Apr 2020
Revision Date	28 May 2020
Major Revision(s)	Version 2.0, 14 Apr 2020: • Whole document; added sub-paragraphs • Para 3.1 (b) & (c): anonymity for blue teams but not observers • Para 3.3.2: added information on scheduling for target system selection phase • Figure 1: replaced PlantViz with PlantViz [OT] in web interface
	Version 3.0, 6 May 2020: Para 3.1.1: Updated red teams' makeup
	Version 4.0, 13 May 2020: • Para 3.1.1: Increased number of red teams to 16 • Para 3.2.2: Added criterion for blue teams • Para 3.4.1 (removed): Removed criteria in which a red team may qualify for 2 CFMs • Para 3.4.4: Updated cash awards for top three red teams • Figure 1: Renamed "Ticketing system" to "Attack logger"
	Version 5.0, 28 May 2020: • Para 3.4.4: Updated scoring criteria for red teams • Para 3.4.6: Added section on reporting of alerts by blue teams

1. Objectives

1.1 CISS2020-OL aims to meet the following key objectives: (a) validate and assess the effectiveness of technologies developed by researchers associated with iTrust[1]; (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 (OpSec).

1.2 In addition, CISS2020-OL will enable red team members to understand approaches for compromising critical infrastructure and hence what protection mechanisms are necessary.

2. History

CISS2020-OL will be the fourth annual cyber defence exercise conducted annually by iTrust. 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. CISS2020-OL will be the first time the event is fully online, where all participants, i.e. red and blue teams, will separately join the event online.

3. Phases in CISS2020-OL[2]

The event consists of the following time-sequenced phases:

Phase I [May 4 - 29, 2020]	:	Participant selection (red & blue teams, observers)
Phase II [June 22 - July 3, 2020]	:	Participant familiarisation (red & blue teams)
Phase III [July 6 - 16, 2020]	:	Target system selection (red teams)
Phase IV [July 27 - Aug 7, 2020]	:	CyberFire (red & blue teams, observers)
Phase V [Q3 – Q4, 2020]	:	Data analysis and reporting

[1] At the time of writing this document, these technologies include automatically generated anomaly detectors using both design and data centric approaches, protection against plant damage, and tools to assist with incidence response

[2] Note that this document is being developed while various technologies for use in CISS2020-OL are under development. Hence, iTrust reserves the right to make changes in the procedure described here in the event all the needed technologies are not available at the time of the CyberFire exercise.

3.1. Phase I: Participant selection

3.1.1. Participation in CISS2020-OL is by invitation only. Participants will be classified into red teams, blue teams and observers. The selection procedure for participants in each category follows:

a) Red teams (comprising 4 - 6 members):
- One from Singapore Ministry of Defence (MINDEF)
- One from Singapore Cyber Security Agency (CSA)
- Up to 14 local and international teams from government organisations, private sector and academia.

b) Blue teams (no limit on the number of members):
- One from iTrust
- 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 maintained throughout.**

c) 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.

3.2. Phase II: Participant familiarisation

3.2.1. All red and blue teams will be offered an online tour of the Secure Water Treatment (SWaT) testbed – one of the target systems (see para 3.3) – and have their questions answered. In addition, they will also be provided:
- information on SWaT, the digital twin, digital twin player, and various anomaly detection and plant safety technologies that will be deployed during the exercise;
- a Frequently Answered Questions (FAQs) (provided separately); and
- access to past data collected from SWaT since 2015, including data collected during CISS 2019.

3.2.2. Blue teams that need to perform hardware installations on SWaT can make a special request. Whenever possible, iTrust will set aside time to supervise the installation by the blue team. Importantly, the blue team shall ensure that:

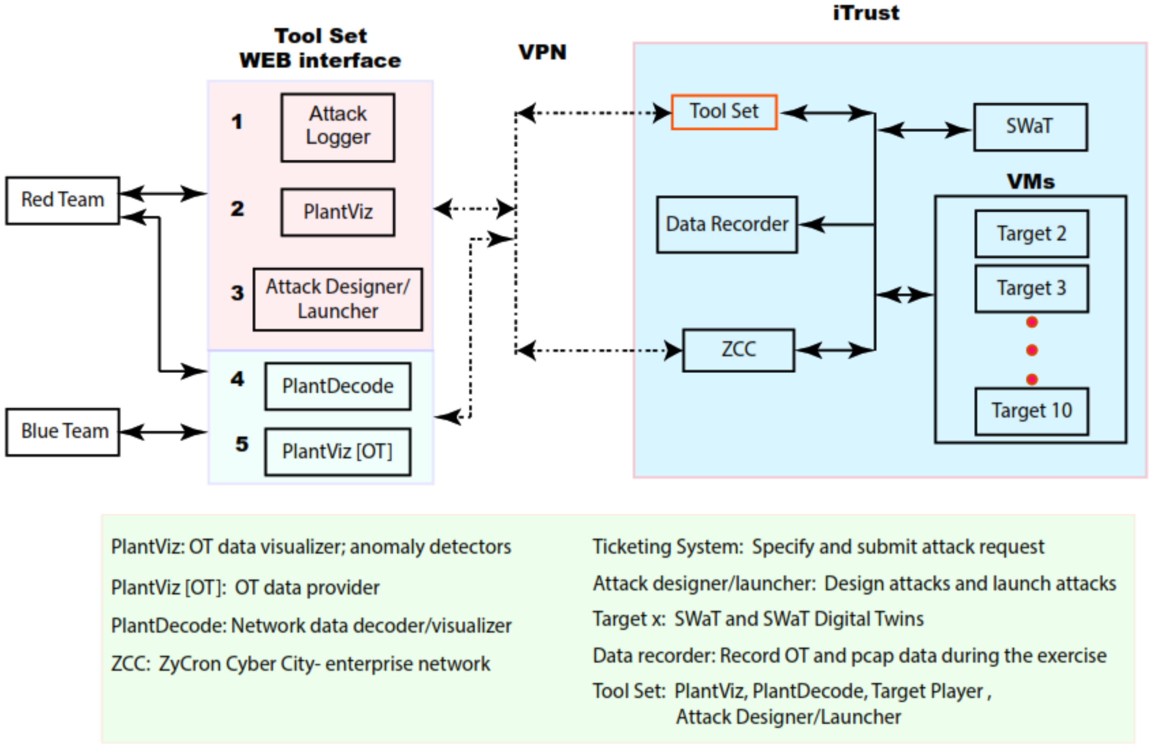
- The installations do not disturb the regular plant operation and interfere with existing iTrust technologies;
- It will make its own arrangements for the data generated by its hardware to be piped to their computers outside of the SWaT during the exercise;
- The installations respond as if in a real-life environment;
- The installations (hard- and software) be completely removed post-exercise and restore SWaT to its original condition. The blue team 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.

3.2.3. iTrust will not provide any additional hardware / software for installation / setting up / GUI display to blue teams, should there be any physical equipment to be set up in SWaT.

3.2.4. For details on attack detection and reporting by blue teams, please refer to paragraphs 3.4.5 and 3.4.6.

3.3. Phase III: Target system selection

3.3.1. Target system selection is the first component of the exercise where red teams are tasked to access the target systems available for attacks. **Target systems consist of SWaT and 9 (actual number to be confirmed) variations of its digital twin.** Figure 1 below captures the interactions among the participants and the target systems. Note that ZCC (see para 3.4.2) will not be available during this phase.



PlantViz: OT data visualizer; anomaly detectors

PlantViz [OT]: OT data provider

PlantDecode: Network data decoder/visualizer

ZCC: ZyCron Cyber City- enterprise network

Ticketing System: Specify and submit attack request

Attack designer/launcher: Design attacks and launch attacks

Target x: SWaT and SWaT Digital Twins

Data recorder: Record OT and pcap data during the exercise

Tool Set: PlantViz, PlantDecode, Target Player , Attack Designer/Launcher

Figure 1: Target systems and tools to be used during CISS2020-OL

3.3.2. A link will be provided on the CISS2020-OL website where red teams can select their 2 hour-timeslot for the target system selection.

3.3.3. Each target system will be kept live during this phase. Red teams will be provided unique URLs to connect to each target system. Data generated by each target system, including OT data captured by the historian and the pcap files, will be piped online and can be viewed through PlantDecode and PlantViz [OT]. All target systems will offer identical, or near identical, user interface.

3.3.4. Each red team will then be asked to make known their target system selection to iTrust; they will then be informed if their selected target system is

SWaT or one of its digital twin variant. This selected target system shall be the one in which they will launch their attacks during the next phase: the CyberFire exercise. **Bonus points will be awarded to the red teams who are able to correctly select the physical SWaT testbed instead of its digital twin.** A red team that selects the digital twin will be granted up to 0.5-CFM (2 hours) to attack SWaT after it has completed launching attacks on the digital twin that it selected, if it so wishes. Note that this 0.5-CFM is included in its allotted 1 CFM slot.

3.4. Phase IV: CyberFire activities

As listed in Table 1 below, the CyberFire activities will be spread over 16 CyberFire modules (CFM.) Each CFM slot is 4 hours and is scheduled from 9am to 1pm and from 2pm to 6pm, GMT+8, 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.

Table 1: CISS2020-OL Schedule for red teams [Team IDs to be filled]

Week 1			**Week 2**	
Date	**CFM slot**		**Date**	**CFM slot**
Mon July 27	1 (AM)		Mon Aug 3	9 (AM)
	SR			SR
	2 (PM)			10 (PM)
Tue July 28	3 (AM)		Tue Aug 4	11 (AM)
	SR			SR
	4 (PM)			12 (PM)
Wed July 28	5 (AM)		Wed Aug 5	13 (AM)
	SR			SR
	6 (PM)			14 (PM)
Thu July 29	7 (AM)		Thu Aug 6	15 (AM)
	SR			SR
	8 (PM)			16 (PM)
Fri July 30	No activity; Public holiday		Fri Aug 7	Data distribution Award announcements

CFM: CyberFire module; red teams attack a target system; SR: System reset (1 hour)
AM slot: 0900 – 1300; PM slot: 1400 – 1800, GMT +8

3.4.1. Attack platform

For added realism, all red teams must attack SWaT by first entering the network via the ZyCron Cyber City (ZCC); they will land in ZCC's corporate network through a VPN connection. ZCC (Figure 2) 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 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 there is no internet access within the ZCC.

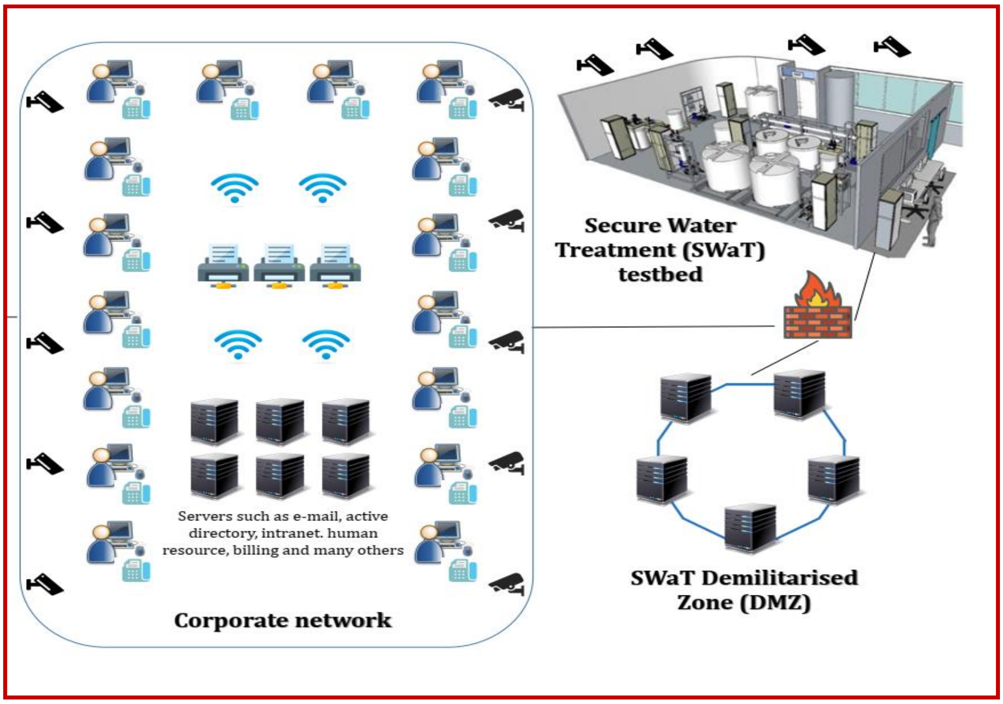

Servers such as e-mail, active directory, intranet. human resource, billing and many others
Corporate network
Secure Water Treatment (SWaT) testbed
SWaT Demilitarised Zone (DMZ)

Figure 2: High-level Architecture of ZyCron Cyber City

3.4.2. Launching attacks

3.4.2.1. Active stage

During a CFM the assigned red team will be asked to demonstrate its attacks and achieve the pre-determined goals (see para 3.4.4 for details on scoring). At this time, the red team is considered "active" and will have online access to its pre-selected target system via a VPN connection. The CFM duration includes, but is not limited to: reconnaissance, designing and launching attacks, interactions with judges (e.g., for Attack Logging; see Figure 1) and taking breaks.

3.4.2.2. Hunting stage

Active teams will be able to design attacks on the target system and launch them remotely using the Attack Designer/Launcher (see Figure 1). This tool is only applicable to SWaT and is meant to facilitate better understanding of the operational technology environment when under attack. The red team will need to "hunt" for its pre-selected target system (in Phase III) before it can begin to launch attacks. As indicated in para 3.4.1, **all red teams must enter SWaT via the ZCC to launch attacks.** Failure to do so and to identify the pre-selected target system will lead to a lower score.

3.4.2.3. Attack launch stage

Prior to launch, the active red team **must do the following throughout its CFM:**

a. Share with iTrust the "live" screen of the computer that is used to launch the attack via an online communication tool (e.g. Skype)[3];
b. Allow iTrust to video record the screen; and
c. Inform judges (1) the intention of the attack; (2) the targeted component(s); and (3) the launch procedure.

Only one attack can be launched on either SWaT or the digital twin variant, but not both at the same time. 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.

3.4.3. Attack monitoring

PlantViz [OT] tool, developed in iTrust, will be accessible to the blue teams and the active red teams. PlantViz [OT] will enable the blue teams and the active red teams to view in real time the state of each state variable in the target system. Any anomaly resulting from the attack, or otherwise (i.e., a false alarm), and reported by one or

[3] 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

more detectors, will also be visible through another PlantViz, **but only to the organisers, observers and judges and not to the red or blue teams.**

3.4.4. Scoring of red teams

The performance of each red team will be assessed in real time by a team of judges consisting of cyber security experts and engineers working in the critical infrastructure domain. All teams that successfully complete the exercise will be given a certificate of participation. Judges during the event 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 awards of S$2,000, S$1,000 and S$500 respectively.** Scoring will be based on the following individual elements.

The total score, *S*, for each attack launched is computed based on five factors *t, p,* a_t, a_{sd} *and b.* These are described in detail below.

$$\text{Total score, } S = t * p * (a_{t1}a_{sd1} + a_{t2}\, a_{sd1} \ldots a_{tn}\, a_{sdn}) + b$$

where:

- *t* = target selection modifier
  - ○ *Selected SWaT (t = 1) or one of the digital twins (t = 0.8) as target system*
- *p* = point of entry modifier
  - ○ *All red teams must attack SWaT by first entering the network via the ZCC (para 3.4.2.); p = 1*
  - ○ *If attempts to enter ZCC are unsuccessful after 30 mins (request to extend to up to 60 will be considered), the team may proceed to attack SWaT or the digital twin (whichever was selected as the target in the selection phase) directly; p = 0.75*
- a_t = an **attack target is** a physical component or parameter in the plant on which the red team wants to launch the attack. An attack target differs from the **attack intention** which is defined as the intended impact as a result of the attack on the target. For example, to cause a water tank to overflow (attack intention), an attacker may choose to launch an attack on

a valve (attack target) by setting it to the CLOSED condition long enough, without getting detected, so that a continuous flow of water into the tank is maintained. The 12 attack targets[4], and their corresponding points, if an attack is successful, in SWaT are:

- Conductivity meter
- Flowmeter
- Historian*
- Water level meter
- Oxidation Reduction Potential Meter
- pH meter
- PLCs
- Pressure meter
- Pumps
- SCADA
- Network switches
- Valves

- a_{sd} = attack success and detection modifier: whether an attack results in an anomaly, and whether the anomaly/attack is detected by any of the installed detectors.
  - *$a_{sd} = s * d$*
  - *If the attack is successful, $s = 1$; else $s = 0$*
  - *d is calculated as:*

↓ d	**s →**	**Attack results in an anomaly**	**Attack does not result in an anomaly**
Anomaly/attack is observed*		0.7	-0.2
Anomaly/attack is not observed*		1	0

**through physical observations of the plant and SCADA screen by plant operator and judges*

- *b* = bonus points for novel attacks (such as the ability to disrupt the anomaly detectors), at the discretion of the judges

[4] Blacklisted attack targets:

- Server rack: The server rack should not be attacked through physical layer
- *Historian: Do not directly try to compromise the historian. We use it to record data for later analysis. You may, however, manipulate data sent to the historian
- General electric supply, fire alarm systems etc.: please do not manipulate the overall setup on a scale that affects more than the testbed setup (e.g., trigger university-wide fire alarm or similar).

3.4.5. Attack detection by blue teams

Throughout the event the blue teams will have VPN access to the active target system i.e., the one selected and in use by the active red team. Blue teams will be able to receive live pcap and OT data for analysis and reporting any anomalies. Blue teams will be encouraged to report any anomaly via PlantViz [OT] using a WEB interface. However, if such reporting is not feasible for any reason then alternate arrangements will be made for reporting anomalies to the event oversight committee. To recap para 3.2.2, **there shall be no efforts made to prevent, halt or thwart any attacks launched by the red teams.**

3.4.6. Reporting of alerts generated by blue teams

It is important for blue teams to note that CISS2020-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 the target system, i.e., SWaT or the digital twin, is not running or is being reset.

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 teams 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.***

3.5. Phase V: Data analysis and reporting

3.5.1 Data from each active target will be recorded and saved in the iTrust data library. Note that part of this data will be from the SWaT testbed while the remaining will be from instances of the digital twins.

3.5.2 Data recorded will consist of measurements from all sensors in each target as well as network packets saved into pcap files. This data will be available publicly via the iTrust data library for use by researchers. Note that the recorded data will contain data mutated by the red teams. Process anomalies generated during the exercise and reported by blue teams will not be a part of the recorded data available publicly.

3.5.3 iTrust will begin data analysis soon after the end of the exercise. The analysis will result in metrics such as the number and types of attacks launched, success rate, detection rate (and false positives), and time taken to detect. Technologies developed in iTrust, and tested during the exercise, will also be evaluated and the outcome included in the event report.

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>