The Fourth International

Critical Infrastructure Security Showdown - Online 2020

Event Plan V6.0

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 interns

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 3
1. OBJECTIVES 5
2. HISTORY 5
3. PHASES IN CISS2020-OL 5
3.1. PHASE I: PARTICIPANT SELECTION 6
3.2. PHASE II: PARTICIPANT FAMILIARISATION 6
3.3. PHASE III: TARGET SYSTEM SELECTION 8
3.4. PHASE IV: CYBERFIRE ACTIVITIES 9
3.4.1. ATTACK PLATFORM 10
3.4.2. LAUNCHING ATTACKS 10
3.4.2.1. ACTIVE STAGE 10
3.4.2.2. HUNTING STAGE 11
3.4.2.3. ATTACK LAUNCH STAGE 11
3.4.3. ATTACK MONITORING 12
3.4.4. SCORING OF RED TEAMS 12
3.4.5. ATTACK DETECTION AND REPORTING OF ALERTS BY BLUE TEAMS 14
3.4.5.1. ATTACK DETECTION 14
3.4.5.2. REPORTING OF ALERTS 15
3.5. PHASE V: DATA ANALYSIS AND REPORTING 15
4. ACCEPTANCE OF TERMS & CONDITIONS 16
5. NOMENCLATURE 17
6. ANNEX A: ATTACK DESIGNER AND LAUNCHER 19

Version History

Version No.	6.0
Effective Date	13 Apr 2020
Revision Date	12 June 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
	Version 6.0, 12 June 2020: • Table 1: Corrected typo on date • Para 3.2.1: Added schedule for participant familiarisation • Para 3.2.4: Added info on hardware setup for blue teams • Para 3.2.5: Added info on remote monitoring by blue teams

	• Para 3.4.5: Combined paras 3.4.5 and 3.4.6 on Attack detection and reporting of alerts by blue teams • Figure 1: Revamped • Figure 3: Added figure for interactions between red/blue teams with CISS2020-OL systems and tools during CyberFire • Figure 4: Added figure for blue teams monitoring their systems' GUI remotely • Para 5: Added nomenclature of tools deployed by iTrust • Annex A: Added description of Attack Designer and Laucnher

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 launch and monitor attacks online, respectively, from wherever they are based.**

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.

Throughout the document there will be several mentions of the tools deployed by iTrust to manage the whole exercise. Red and blue teams are encouraged to familiarise themselves with these terms by referring to paragraph 5.

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 makeup of participants in each category follows:

a) Red teams (up to 6 members):
   - One from Singapore Ministry of Defence (MINDEF)
   - Up to 15 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. The schedule is as follows:
   - Blue Teams: 22 Jun, 9am – 11am, SUTD, Lecture Theatre 3 (Building 2, Level 4)
   - Red Teams: 29 Jun, 4pm – 6pm, online

3.2.2. 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.

3.2.3. Blue teams that need to perform hardware installations on SWaT are provided slots to do so (3.2.4.) 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.

3.2.4. 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. Each blue team will be provided up to 3 slots of 2 hours per slot during working weekdays to install its hardware.

3.2.5. Blue teams' systems will be connected to iTrust's TAP switch to receive pcap data from Zycron Cyber City and SWaT (see Figure 4). Two Ethernet cables will be provided for this purpose. As blue teams will not have physical access to SWaT, they will need to set up remote monitoring capabilities to view their systems' GUI off-site over SUTD's WiFi.

3.2.6. For details on attack detection and reporting by blue teams, please refer to paragraph 3.4.5.

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 3.4.1) will not be available during this phase.

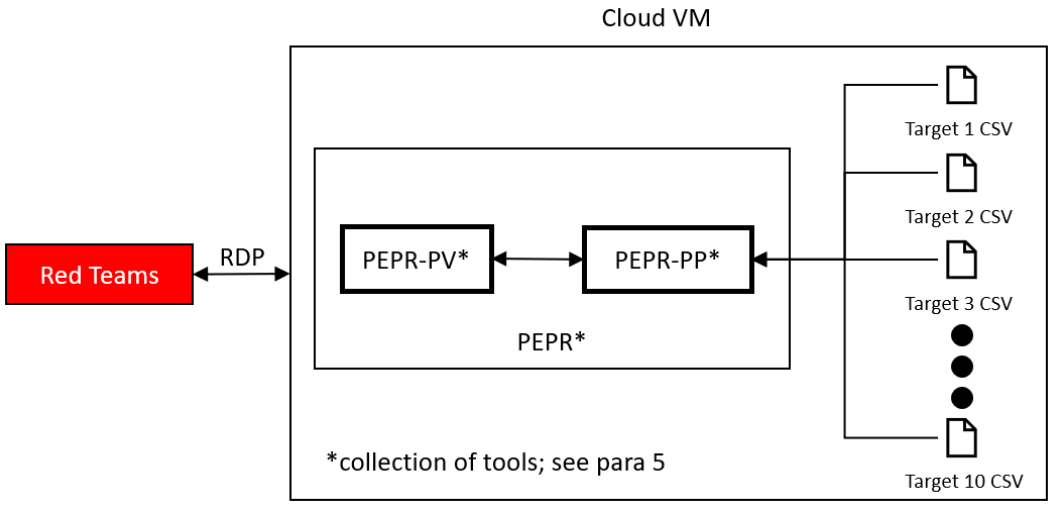


Figure 1: Interactions between red teams and CISS2020-OL system and tools during target selection phase

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. Red teams will be provided unique credentials to connect to Cloud VM 30 minutes before their target selection timeslot. OT data captured by the historian by each target system, will be available on the Cloud VM and can be viewed through PEPR-PV and PEPR-PP.

3.3.4. Each red team will then be asked to make known their target system selection to iTrust via email (to itrust@sutd.edu.sg), **within 2 hours** from the end of their target selection slot; 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.**

3.3.5. A red team that selects the digital twin will be granted up to 0.5 CyberFire modules (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

The CyberFire activities will be spread over 16 CFM (Table 1). Each CFM slot is 4 hours and is scheduled from 9am to 1pm or 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 29	5 (AM)		Wed Aug 5	13 (AM)
	SR			SR
	6 (PM)			14 (PM)
Thu July 30	7 (AM)		Thu Aug 6	15 (AM)
	SR			SR
	8 (PM)			16 (PM)
Fri July 31	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.

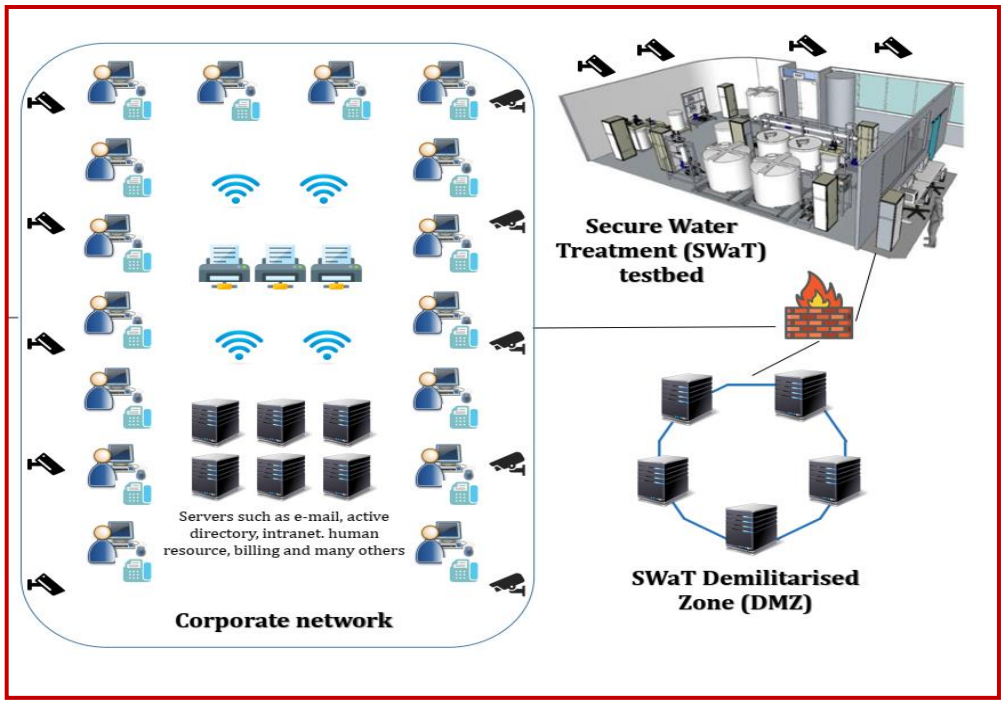


Figure 2: High-level Architecture of ZyCron Cyber City

3.4.2. Launching attacks

3.4.2.1. Active stage

During a CFM the active 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 3) and taking breaks.

3.4.2.2. Hunting stage

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. If, during its CFM slot, attempts to penetrate into SWaT network through ZCC corporate network are unsuccessful after 30 mins (request to extend to up to 60 mins will be considered), the team may proceed to attack SWaT or the digital twin (whichever was selected as the target in the selection phase; see also scoring criteria.)

ZCC is built with typical enterprise vulnerabilities that exist in many organisations. The red team will first have to "hunt" for these vulnerabilities and compromise them before using them to "hop" deeper into the network and eventually locate SWaT/digital twin in the OT network.

3.4.2.3. Attack launch stage

Active teams can choose to design attacks on the target system and launch them using the Attack Launcher (see Figure 3 & Annex A), or use their own attack vectors. The Attack Launcher is only applicable to Digital Twin and is meant to facilitate better understanding of the operational technology environment when under attack.

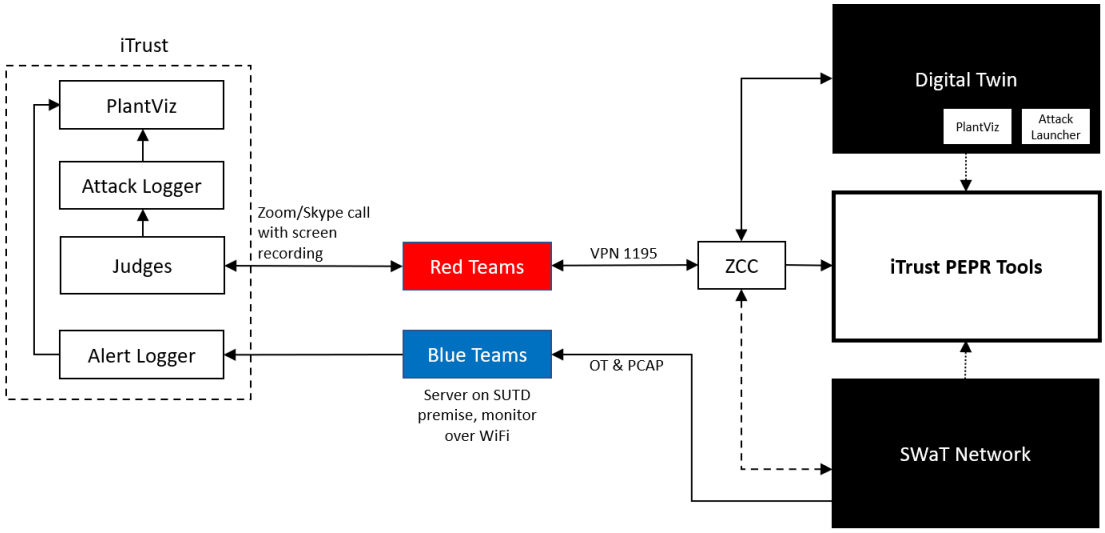


Figure 3: Interactions between red/blue teams with CISS2020-OL systems and tools during CyberFire

Prior to launching its attacks, 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

Blue teams and the active red teams will be able 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 more iTrust detectors, will be visible **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.

[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

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.

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

where:

- *t* = target selection modifier
  - *Selected SWaT (t = 1) or one of the digital twins (t = 0.75) 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 in parentheses, if an attack is successful, in SWaT are:
  - Conductivity meter (300)
  - Flowmeter (200)
  - Historian* (100)
  - PLCs (100)
  - Pressure meter (200)
  - Pumps (200)

[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).

- Water level meter (200)
- Oxidation Reduction Potential Meter (300)
- pH meter (300)
- SCADA (100)
- Network switches (100)
- Valves (200)

- 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

3.4.5. Attack detection and reporting of alerts 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.

3.4.5.1. Attack detection

Throughout the event the blue teams will monitor their systems remotely (Figure 4 next page). Post-event, blue teams will be given pcap and OT data captured for analysis. To recap para 3.2.2, **there shall be no effort made by the blue teams to prevent, halt or thwart any attacks launched by the red teams.**

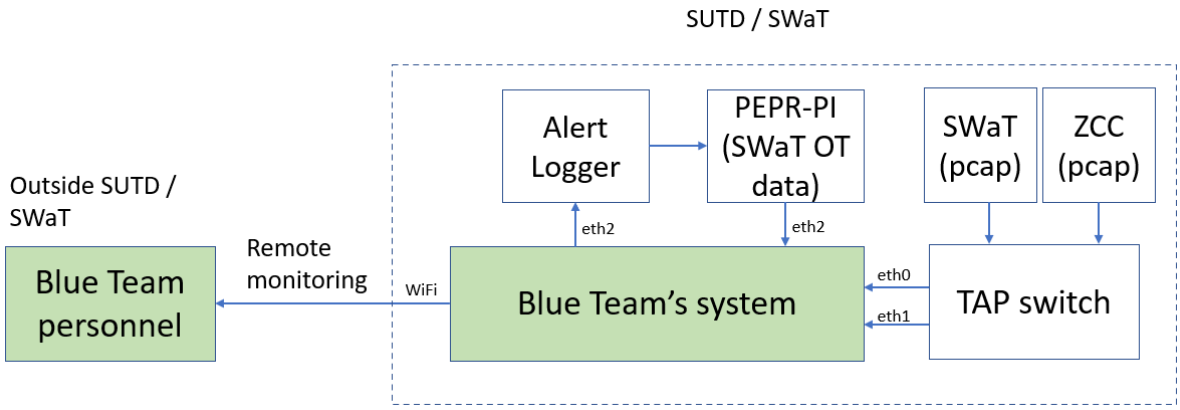


Figure 4: Blue teams monitoring their systems' GUI remotely

3.4.5.2. 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) PEPR-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 PEPR-PV for automatic logging and visual alerts; or
b) Alert logger: a simple password-protected web interface to log a time-stamped alert each time the blue team detects an attack.

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>

5. Nomenclature

Alert Logger: Automates the process of logging and sending time-stamped alerts by blue teams to iTrust

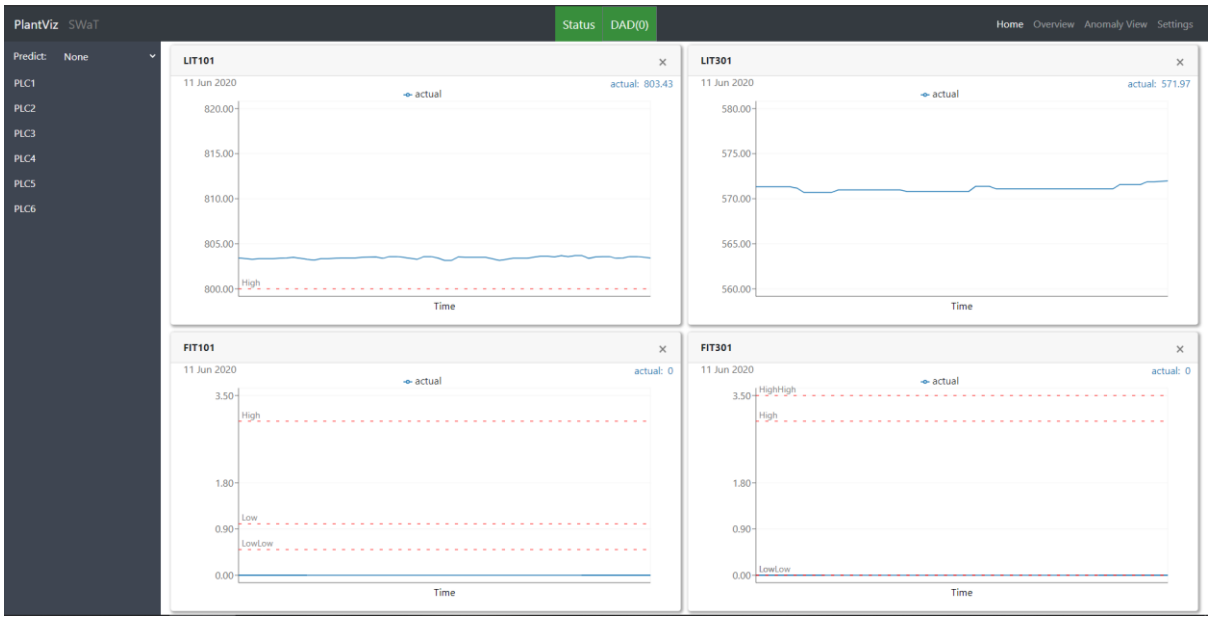
Attack Launcher: Optional platform for red teams to select and launch attacks

Attack Logger: Communicate attack intentions & steps to White Team & judges and log attacks as they happen

PEPR: Collection of tools (PlantPlayer (PP), PlantViz (PV) and PlantIO (PI)) that allows players to play back past historical data to enable blue teams to test their own detection systems

PEPR-PP: Tool to playback past historical data

PEPR-PV: Visualisation tool for live, prediction, and anomaly data from detectors.



PEPR-PI: A suite of tools that allows detectors to save, publish and playback live, prediction, and anomaly data for detector performance analysis. The data which is saved or published can be used by other tools on the same network.

6. Annex A: Attack Designer and Launcher

Attack Designer[5]

Attack Designer is a tool to design attacks on any of the components in the Digital Twin for SWaT. Attacks are of two types: atomic and multi-point. An atomic attack is an attack on a selected component of SWaT, e.g., LIT101. A multi-point attack is a combination of two or more atomic attacks. Both continuous and discrete valued states can be the target of the attacks. Attacks designed are saved in an attack database and can be launched on the twin by the Attack Launcher.

Version 1.0 of the Attack Designer can be used to design the following attack types:

Attack Code	Code expansion	Description
AR	ARP spoofing	Address Resolution Protocol attack
CL	Clone	State of a component clone a similar component
CO	Constant	Fix a measurement to a constant value
FB	Fixed Bias	Add a fixed bias to a state measurement
GB	Gradual Bias	Add a variable bias to a state measurement
CH	Chatter	Cause an actuator to change its state at a given frequency
DL	Delay	Delay a measurement from reaching its destination
ML	Malware	Introduce malware in a selected component of the twin
PM	Parameter	Change one of the control parameters used by a PLC in the twin
RP	Replay	Replay the state of a selected state variable

The following parameters are associated with the attacks.

- **Target**: The component whose state is to be manipulated

[5] Attack Designer will be available in the Digital Twin for SWaT in Q3 of 2020.

- **Type:** Attack type (as mentioned in the table above); attack types available depend on the target
- **Source:** Source component at which the target component state is to be manipulated
- **Destination:** Destination component where the manipulated state is to be sent
- **State:** Manipulated value
- **Frequency:** Rate at which the state of an actuator is to be changed in chatter attack
- **Duration**: Attack duration

Attack Launcher[6]

Digital Twin for SWaT contains two attack launchers referred to as AL-OT and AL-PCAP. Both launchers are available with their own user interfaces. These two launchers are described next.

As the name suggests, AL-OT enables a twin user to launch attacks designed using the Attack Designer. AL-OT has two components: Launcher and Proxy. The Launcher receives attacks designed using the Attack Designer and displays these on an Aattack Desk from where attacks can be selected for launch, activated, and deactivated. The Attack Proxy is a separate module that interacts with the Launcher to obey attack commands. Each command is created by the Launcher to implement an attack selected by the user managing the Attack Desk.

AL-PCAP launches attacks by manipulating packets flowing across the twin communications network. The key difference between AL-PCAP and AL-OT is in how the state of the twin s manipulated. While AT-OL manipulates the state directly on values available just before they are sent to the destination via the send-string() command in PyZmq, AT-PCAP manipulates the network packets. The ability to directly manipulate packets makes AL-PCAP more versatile launcher than AL-OT.

[6] AL-PCAP will be available for use during CISS-2020-OL. AL-OT will be available in Q3 of 2020.