
# Red Week Technical Report

**Sponsors**:

National Research Foundation, Singapore

Ministry of Defence, Singapore

**Date**:

6 Sept to 10 Sept 2021

**Report by:**

Francisco FURTADO, Andy TAY, Ivan LEE, Reuben CHNG, ONG Wee Keat, LOH Zhi Qin

**Organisers:**

Ministry of Defence, Singapore

iTrust, Centre of Research in Cyber Security

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# 1. Introduction

The Critical Infrastructure Security Showdown 2021 (CISS2021-OL), conducted over two weeks from 6 to 17 Sep 2021 at the Singapore University of Technology and Design (SUTD), was the fifth run of iTrust's technology assessment exercise.

CISS2021-OL was sponsored by the Ministry of Defence, Singapore and the National Research Foundation.

# 2. Objectives

CISS2021-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 against cyberattacks

c. understand composite Tactics, Techniques and Procedures (TTP) for enhanced Operation Security.

In addition, CISS2021-OL will enable both Red and Blue Team members to understand approaches for compromising and defending critical infrastructure and to put in place the necessary protection mechanisms.

This report is focused on the Red Week Technical Report.

# 3. History & Modality

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 launched and monitored attacks online from wherever they were based.

CISS2021-OL retained the online platform modality, with the following additions:

a. World Wide Web as the entry point
b. Water Distribution (WADI) testbed and SWaT/WaDi Digital Twin as an 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

[1] 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.

f. Higher score for Red Teams that use reflector servers to mask their identity
g. Prize money for Red Teams doubled

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

a. Red Week (6 to 11 Sep):

Each Red Team was given 5 hours to launch attacks on the platform and gain points when they met attack objectives. Blue Teams Vendors were commercial companies who had installed their products to detect Red Teams' attacks. Red Teams' TTP were captured during this week. Red Teams and Blue Team Vendors' participation were by invitation only.

b. Blue Week (13 to 17 Sep):

A composite Red Team was formed by various organisations to launch attacks on the platform, which was being defended by Blue Teams that comprised of Critical Information Infrastructure (CII) operators and regulators ("CII Blue Teams"). Each CII Blue Team was given one slot of 8 hours to respond to the attacks and defend the platform. The five CII Blue Teams' participation was by invitation only.

There were four classifications of participation in CISS201-OL. The makeup of participants in each category follows:

1. Red Teams (up to 4 members):
   - Up to 10 local and international teams from government organisations, the private sector and academia.
   - Stage 1 was organised in July to admit the top 10 Red Teams into the Finals (Red Team Exercise from 6 to 10 Sep).

2. Blue Team Vendors (BTVs):
   - Commercial vendors were invited based on their past performance in similar events and nominations by Singapore Government agencies.

3. IHL Anomaly Detection Mechanisms (ADMs):
   - Various anomaly detectors from iTrust
   - Academia from centres around the world that have cyber-security as their prime focus and have demonstrated a research record in securing critical infrastructure.

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

5. Observers:
   - Singapore Government agencies and their invitees. iTrust executed the event online, where any authorised observer could track the progress - in terms of attacks launched and detected - of the event.

# 4. Phases in CISS2021-OL Red Week

| Phase | Date | Details | Involvement |
|---|---|---|---|
| **Stage 1** | 5 – 16 Jul | Stage 1 (3 hours per team) to admit 10 Red Teams to the final round | Red Teams |
| | 21 Jul | Red Team Finalists for CISS2021-OL were published | Red Teams |
| **Red Team Preparation** | 30 Jul | Briefing for Red Team Finalists | Red Teams |
| | 4 – 13 Aug | Familiarisation: Testing VPN, RDP, attack tools | |
| | 23 Aug | Submission of VMDK | |
| **Blue Team Preparation** | 10 Aug | Blue Team Vendor Briefing | Blue Team Vendors |
| | 16 – 31 Aug | Onsite deployment, baselining of products | Blue Team Vendors |
| **Opening Ceremony** | 3 Sep | Welcome Address by organisers<br>Tour of Testbeds | All |
| **CISS2021 Finals** | 6 to 10 Sep | Red Team Exercise | Red Team, Blue Team Vendors |

## 4.1. Stage 1 [5 to 16 Jul]

A total of 17 red teams registered for CISS2021-OL. As only 10 Red Team slots were available in the Finals, Stage 1 was organised to shortlist the 10 best-performing Red Teams into the Finals.

Each Red Team was given 3 hours in Stage 1 to meet a set of attack objectives. The top 10 teams that achieved these objectives in the fastest time were admitted into the finals.

## 4.2. Red Team Preparation [30 Jul to 23 Aug]

All Red Teams were provided with the following:

- Information on the exercise platform including the simulated World Wide Web (sWWW), Zycron Cyber City (ZCC), 2 branches of water treatment plants, 2 branches of water distribution plants, various anomaly detection and plant safety technologies.
- A process architecture, network diagram and operation manual of each plant.
- 4 Kali VMs in the Form Up Area (FUA) with administrative rights
- 4 Reflector VMs in the sWWW with administrative rights
- OpenVPN credentials with a 90 min familiarisation period to test their VPN connection, tools installation and enumeration
- Option for customised VM to be installed instead of the Kali VM
- Past CISS reports (2016, 2017, 2019, 2020)
- Out-of-bounds information
- Rules of Engagement & Scoring

## 4.3. Blue Team Preparation [10 Aug to 31 Aug]

A total of 5 commercial vendors participated in CISS2021-OL as Blue Teams, referred to as Blue Team Vendors (BTVs) 1, 2, 3, 4 and 5. All BTVs were provided with the following:

- Information on exercise platform including the sWWW, ZCC, 2 branches of water treatment plants, 2 branches of water distribution plants, various anomaly detection and plant safety technologies.
- A process architecture, network diagram and operation manual of each plant.
- Out-of-bounds information.
- Reporting of alerts from their system.
- 2 full working days to set up their hardware for attack detection, remote monitoring and automatic reporting of alerts.
- 3-hour baselining period.

## 4.4. CISS2021-OL Red Team Finals

The CISS2021-OL Red Team Finals was spread over 10 Red Team Slots from 6 to 11 Sep (Mon – Fri). The duration of each slot was 5 hours and was scheduled from 0900 hrs to 1400 hrs or from 1500 hrs to 2000 hrs daily, with a one-hour break in between for system reset.

# 5. Exercise Platform

All red teams were required to attack the OT network by first entering Zycron's corporate network via sWWW. They would land in the FUA through a VPN connection. Reflectors were available in the sWWW for the teams to remote in and mask their identity. For added realism, various internet services were created in the sWWW like DNS and NTP service. Web applications like vendor and provider websites were also included (Figure 1).

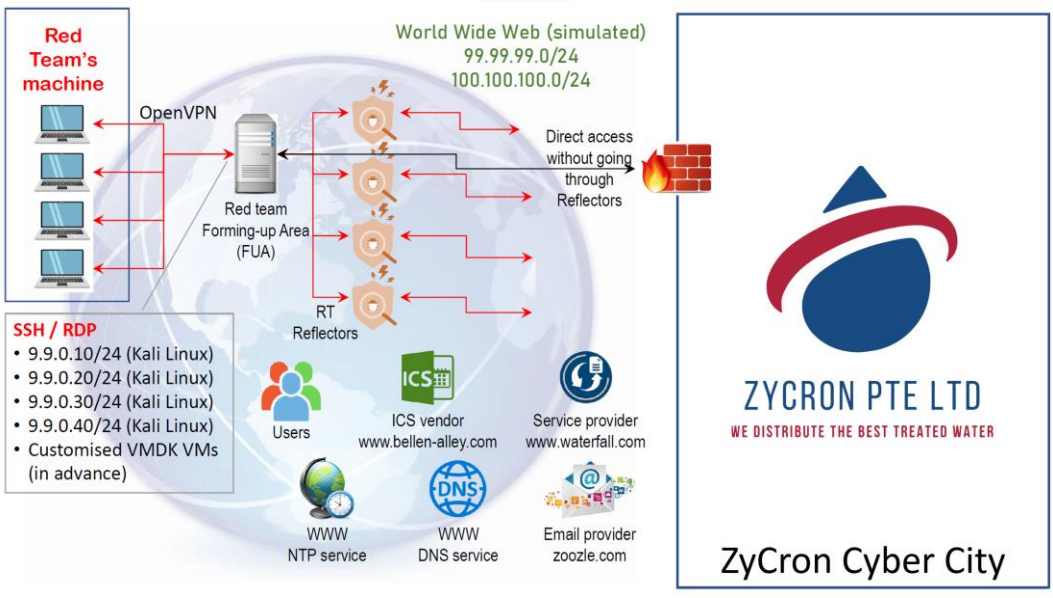


*Figure 1: High-Level Architecture of Exercise Platform and sWWW*

Zycron Cyber City (ZCC) is a full-fledged virtual organisation comprising 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 were also crafted and included in ZCC. As an IT environment, ZCC was not set up with best practices i.e., it was intentionally built with minimum security features and contained vulnerabilities for red teams to explore and exploit. There was no internet access within the ZCC. A high-level architecture of ZCC is given in Figure 2 below.

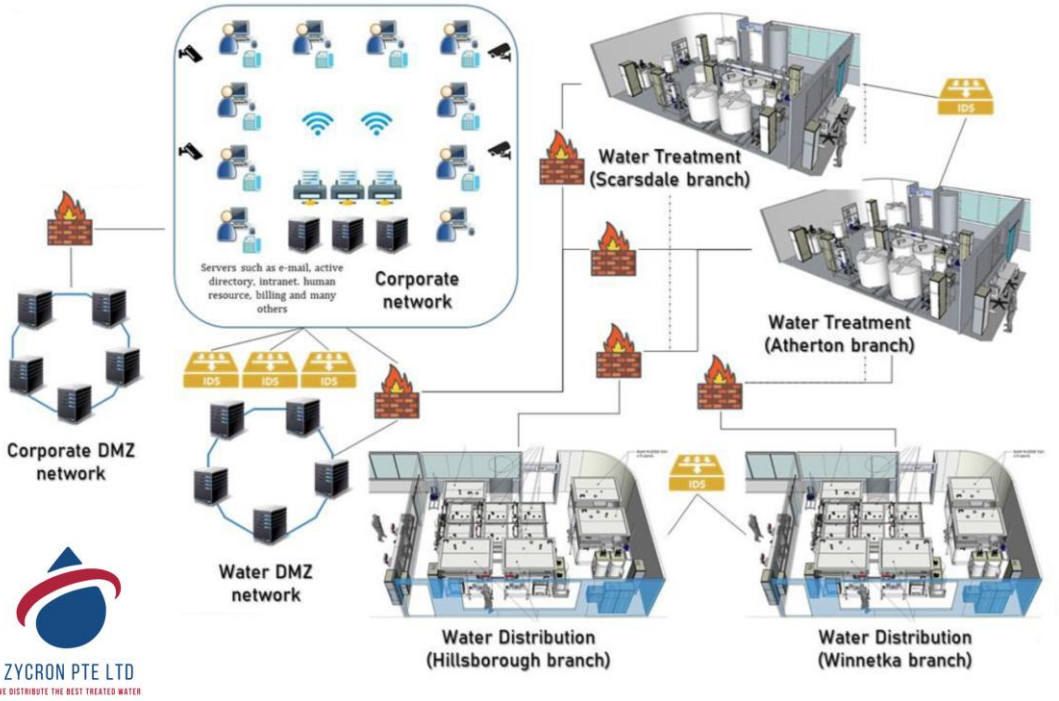


*Figure 2: High-Level Architecture of ZCC*

## 6. Launching attacks

Red Teams designed and launched attacks on the attack platform for 5 hours. Before launching attacks, the team had to comply with 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)[2];

b. Allow iTrust to record their screens (video and audio); and

[2] 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

c. Inform judges of (1) the intention of the attack; (2) the targeted component(s); and (3) the launch procedure.

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

## 7. Attack monitoring

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

## 8. Scoring of Red Teams

The performance of Red Teams was 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, were allowed i.e., an attack could only begin after the previous one had ended or was aborted. Judges scored 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. The top three Red Teams received cash prizes of S$4,000, S$2,000 and S$1,000 respectively. The total score, S, for each attack launched was computed based on five factors:

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

where:

- A = Attack Score
    - Achieving different attack objectives will be rewarded with 100 – 400 points, depending on their difficulty
- 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 the OT Network are unsuccessful after 60 mins (request to extend to up to 90 will be considered), the team may request to be teleported to attack SWaT or the digital twin directly
    - T = 0.5 and E=1.0 if teleport is required; else, 1.0
- I = IDS penalty

- IDS is installed in ZCC and the OT Network. 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 500 points
  - Suricata and Zeek IDS have been deployed

# 9. Attack Detection

Blue Team Vendors (BTV) were briefed that CISS2021-OL would be conducted to simulate attacks on a live city-scale plant. Hence, it was assumed that the security systems deployed by each BTV were operational throughout the exercise.

Throughout the exercise, the Blue Teams monitored their systems remotely. Post-event, Blue Teams were given the attack data captured for analysis.

# 10. Reporting of Alerts

Alerts generated by the security system deployed by a BTV or ADM had to be reported *immediately* and *automatically* to the reporting system via Syslog. While each BTV and ADM would be provided with all event data, e.g., Historian data, at the end of the event, they were not expected to analyse alerts generated during the event. BTVs and ADMs were requested to submit their analysis of their product to iTrust for post-CISS analysis.

# 11. Data Analysis and Reporting

Data from each Red Team session were recorded and saved in the iTrust data library. These consisted of measurements from all sensors in the OT network as well as network packets saved into pcap files. The recorded data contains data mutated by the Red Teams.

# 12. IHL Detectors

## 12.1. AEGIS

*Background*

Automatic Extensible Generic Invariant-based Security (AEGIS) is an attack detection tool that intends to augment the usability of DAD by automating the process of invariant creation. It comprises an algorithm designed to be generic and universal for various types of CPS, offering the option of plant-specific customisation for users.

*Technology Description*

The first step in the automation using AEGIS' algorithm hinges on the idea of reading the connections between the components of the plant from its CAD (Computer-aided Design) file or P&ID (Piping and Instrumentation Diagram). Based on encoded physics principles, the algorithm then automatically generates the rules that the associated sensor-actuator sets must follow for the proper operation of the system. These rules, called invariants, are created using similar logic as followed by DAD.

When the tool is in operation, it keeps checking the incoming sensor and actuator readings to determine whether the actual system behaviour is following its expected performance. The violation of the invariants could be a sign of the presence of process anomalies, which could be occurring due to attacks.

The tool is modular in its architecture and allows plant operators to tune the generalised design parameters and device-specific constants to tailor the detector for their systems.

## 12.2. AICrit

*Background*

AICrit's intelligence integrates the design knowledge and machine learning algorithms into one versatile solution for automated process monitoring and threat detection in the operational Industrial Control Systems (ICS).

*Technology Description*

AICrit for anomaly detection in ICS is a unified framework for real-time process monitoring to preserve the control behaviour integrity of the ICS. It precisely learns the normal spatiotemporal relationship among the set of highly correlated components through the application of machine learning algorithms (data-centric approach) and with a considerable amount of design knowledge (design-centric approach). The process involved in the design of the unsupervised detector presented here is of two-folds. One is modelling the normal behaviour of continuous-valued state variables (sensors) through the temporal dependencies to forecast their behaviour with minimal error. The second is modelling the higher-order and non-linear correlation among the discrete and continuous type state variables (cross-correlation among the sensors and actuators) during the normal plant operation. By combining these two, the functional dependencies of the sensors and actuators are monitored continuously, which increases the confidence in discovering and reporting a wide range of anomalies during the discrepancies in the expected and actual behaviour of ICS.

## 12.3. FLBI

*Background*

FLBI is a blockchain-based system that provides data integrity and real-time anomaly detection of sensor values. FLBI is deployed in SWaT to detect anomalies during the CISS event.

*Technology Description*

In SWaT, sensor values are measured and stored into the historian through six PLCs which are responsible for each stage of the water treatment process. At the high level, FLBI collects sensor values directly from PLCs and store the hashes of these values inside the blockchain. We provide the data integrity of the historian by periodically comparing the hashes of the sensor values from the historian with the ones from the blockchain.

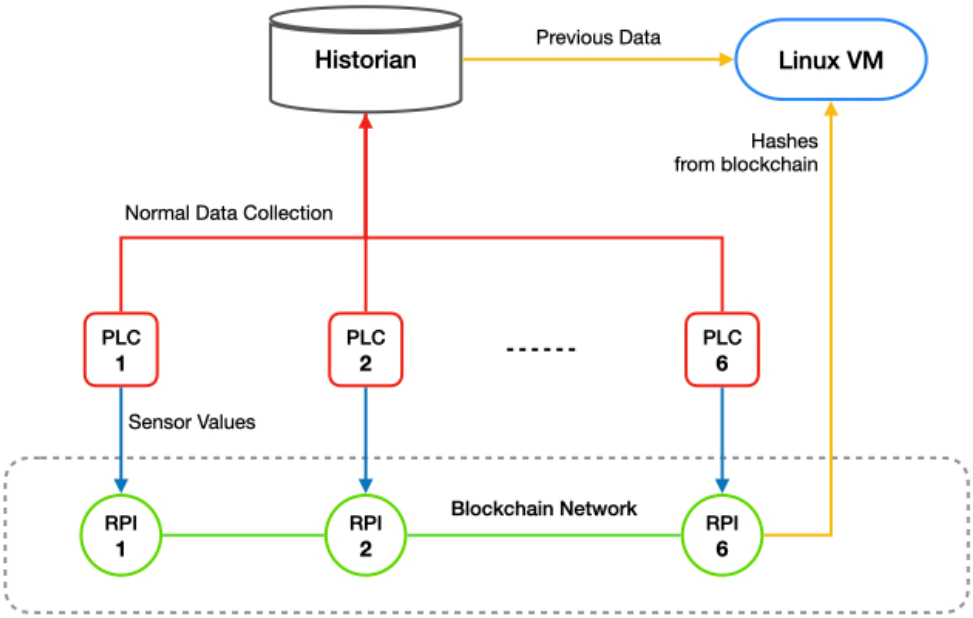


*Figure 3: FLBI deployment in SWaT.*

We set up a network of six RPI inside the plant network and made each RPI connected to a different PLC physically through the ethernet cable. We run a blockchain on top of the RPI network to store the hashes of sensor values and run anomaly detections using the Smart Contract. We used two different blockchains: Ethereum and Hyperledger Fabric. Sensor values from each PLC are collected by a respective RPI and stored inside the blockchain. If the Smart Contract finds an anomaly in sensor values (such as value too big or small), It will generate an alert and report it to the PlantViz system of SWaT.

For periodic data integrity checking, we used a Linux VM inside the SWaT network.

On that VM, we run a script that queries previous data from the historian and compares it with the hashes from the blockchain periodically. If any data is incorrect or missing, it generates an alert and reports it to the PlantViz system.

## 12.4. ATTester

*Background*

The attestation tool is a mechanism, which specifically addresses the problem of attesting the integrity of the PLC code. The attestation techniques typically can be categorized into

three types-software-based attestations, hardware-based attestation, and physical attestation. Since SWaT does not provide the hardware for hardware-based attestation, and access to the firmware, a practical remote attestation solution is used where the mechanism only requires all sensor readings, actuator states, and variables concerning PLC state as input.

*Technology Description*

Firstly, the faithful offline copies of its PLC programs are written in python. This code will generate the corresponding actuator commands for the given sensor readings, actuator states, and variables. Based on the inputs from the real system, the ATTester tool can predict the state of the actuators. Then, the prediction states and the state in the future are checked and will raise alarm(s) if these two values are not consistent.

## 12.5. AD_Check

*Background*

Axiomatic Design invariant checker (AD_Check) is a supervised machine learning design-centric attack detection algorithm developed by researchers for the NSOE project, "A two-track approach to CPS Reconnaissance: causal-graphs and axiomatic design".

*Technology Description*

AD_Check detection system invariants are derived from customer requirements using axiomatic design theory which is a design science discipline, instead of from mathematical equations or formulas. The algorithm learns the label of each scenario based on the learning dataset provided by the designer or developer. According to our research results, the algorithm gives 100 per cent accuracy in its predictions. AD_Check can detect anomalies for design-based discrete systems like motorised valves and pumps in SWaT and WADI testbeds. This algorithm is particularly effective and efficient for invariants that consist of more than five devices. More information about this research can be found in the papers, "Towards Systematically Deriving Defence Mechanisms from Functional Requirements of Cyber-Physical Systems" and "Deriving defence mechanisms for critical infrastructure using axiomatic design principles".

## 12.6. Secure Digital Water Twins (SDWT)

*Background*

SDWT is the digital twin to protect critical water infrastructures developed by a team of researchers in NTU. SDWT shall leverage on advanced machine learning algorithms for predictive analysis, to provide effective safeguards against operational anomalies and cyber-attacks in critical water treatment infrastructures. The current SDWT is built on ThingWorx platform based on value streams from SWaT testbed, and it is iteratively improved with more data from SWaT.

*Technology Description*

The original SDWT on ThingWorx divides sensors/actuators into three groups. Some sensors such as water level values can be predicted by scientific expression because of certain relationship between water level, flow rate, time and tank size. Actuators only show binary values, therefore can be predicted according to logic relation in RSLogix5000. For rest of sensors like PH of water, we build machine learning models with Python based on historical data.

However, to better integrate SDWT with PlantViz, only the Python-based detectors are used in CISS. For other sensors/actuators, corresponding machine learning models are trained urgently without fine tuning, so the performance may be affected.

For each target, only important features are chosen to form sequential sample inputs, and each sensor/actuator has its own detector. The algorithm will collect data as inputs to predict values at next timestamp. Though upgraded RAMs are replaced for the host, the delay due to multiple models still exists for five seconds.

SDWT has three steps to detect anomalies. First is the valid input judgement, which will send alarms directly when it receives bad inputs. The other two are judgments based on threshold for specific difference. Our SDWT is a novel technology because our machine learning models can output the prediction together with its uncertainty. The uncertainty here represents possible error of the prediction, so the algorithm may allow larger difference between the prediction with the measurement when uncertainty is large. Thus, the threshold for the difference is adaptive instead of fixed.

In addition, special cyber-attacks are taken into consideration. Our detectors calculate cumulative error with the uncertainty from model outputs and the difference between prediction and measurement based on Gaussian assumption. With our cumulative error threshold, well-designed attacks such as gradual attacks can be detected as well.

# 13. Evaluation of Defence Mechanisms

The defence mechanisms were evaluated based on the total OT attacks detected on the exercise platform at each Red Team session. IT actions were not considered in the evaluation. During the event, Blue Teams sent real-time alarms to an Alert Logger when their defence mechanisms detected an attack. These alarms were then evaluated along a survey which was sent out to each Blue Team to indicate 'Yes' (Y) implying that an attack was detected and 'No' (N) implying that an attack was not detected. All detected attacks have been documented down with evidence.

The IHL detectors, with the exception of FLBI, were subscribed to the CloneHistorian to receive the process data. This data was used to detect process anomalies. During the analysis, it was found that the data published by the CloneHistorian was faulty. This was unfortunate and so the IHL detectors are not evaluated in this report.

The BTVs were connected to a network Test Access Point (TAP) which provided network packets of the systems which were used for attack detection. Though there were 6 BTVs that participated and connected their systems, only 3 had provided their analysis in the format and time required for this report.

The remaining 3 BTVs were evaluated using the Sep 6 and 8 morning sessions. **These sessions were selected as they contained the greatest number of OT attacks.**

## 13.1. OT Attacks Captured

From the 2 Red Team sessions selected, a total of 27 OT anomalies were captured. In the 6 Sep session, there were a total of 18 anomalies, and 9 anomalies for the 8 Sep session. These anomalies are listed in

Table  below.

*Table 1: Attacks used in the analysis of detectors*

** - Attacks while PlantProtect turned on active defence*
*No. 1 to 18: 6 SEP, AM. No. 19 to 27: 8 SEP, AM.*

| Attack No. | Description of Attacks |
|---|---|
| 6 Sep (Team A) | |
| 1* | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 CLOSE. |
| 2* | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 CLOSE. |
| 3* | Scarsdale Water Treatment Plant<br>Manipulation of dosing pumps: P201, P202, P203, P204, P205, P206, P207, P208 all STOP.<br>Spoof values of FIT201, AIT202 & AIT203.<br>Manipulation of motorised valve: MV201 &MV301 OPEN. |
| 4* | Scarsdale Water Treatment Plant<br>Manipulation of UF backwash Pump: P602 STOP.<br>Manipulation of motorised valve: MV301 &MV303 CLOSE. |
| 5* | Scarsdale Water Treatment Plant<br>Manipulation of UF Feed Pump: P301 & P302 RUN.<br>Spoof values of UF Feed water level meter: LIT301.<br>Manipulation of motorised valve: MV301, MV302 & MV303 CLOSE. |
| 6* | Scarsdale Water Treatment Plant<br>Manipulation of UF Feed Pump: P301 & P302 RUN<br>Spoof values of UF Feed Water Level Meter: LIT301.<br>Manipulation of motorised valve: MV301, MV302 CLOSE while MV303 OPEN |
| 7* | Scarsdale Water Treatment Plant<br>Manipulation of High-Pressure Pumps: P501, P502 RUN.<br>Manipulation of RO Permeate Pump: P601 RUN.<br>Manipulation of motorised valve: MV501 & MV504 CLOSE while MV502 & MV503 OPEN. |
| 8* | Scarsdale Water Treatment Plant<br>Manipulation of High-Pressure Pumps: P501, P502 RUN.<br>Manipulation of RO Permeate Pump: P601 RUN.<br>Manipulation of UF backwash Pump: P602 RUN.<br>Manipulation of CIP Pump: P603 RUN.<br>Manipulation of motorised valve: MV501 & MV504 CLOSE while MV502 & MV503 OPEN. |
| 9 | Scarsdale Water Treatment Plant<br>Manipulation of dosing pumps: P201, P202, P203, P204, P205, P206, P207, P208 all STOP.<br>Spoof values of FIT201, AIT202 & AIT203.<br>Manipulation of motorised valve: MV201 &MV301 OPEN. |
| 10 | Scarsdale Water Treatment Plant<br>Manipulation of UF Feed Pump: P301 & P302 RUN. |

| | |
|---|---|
| | Spoof values of UF Feed water level meter: LIT301.<br>Manipulation of motorised valve: MV301, MV302 & MV303 CLOSE. |
| 11 | Scarsdale Water Treatment Plant<br>Manipulation of High-Pressure Pumps: P501, P502 RUN.<br>Manipulation of RO Permeate Pump: P601 RUN.<br>Manipulation of UF backwash Pump: P602 RUN.<br>Manipulation of CIP Pump: P603 RUN.<br>Manipulation of motorised valve: MV501 & MV504 CLOSE while MV502 & MV503 OPEN. |
| 12 | Scarsdale Water Treatment Plant<br>Manipulation of RO Permeate Pump: P601 DISABLED. |
| 13 | Scarsdale Water Treatment Plant<br>Manipulation of RO High Pressure Pump: P501 DISABLED. |
| 14 | Scarsdale Water Treatment Plant<br>Manipulation of RO High Pressure Pump: P502 DISABLED. |
| 15 | Scarsdale Water Treatment Plant<br>Manipulation of RO Feed Pumps: P401 & P402 DISABLED.<br>Manipulation of Dosing Pumps: P403 & P404 DISABLED. |
| 16 | Scarsdale Water Treatment Plant<br>Manipulation of UF feed pump: P301 & P302 DISABLED. |
| 17 | Scarsdale Water Treatment Plant<br>Manipulation of dosing pumps: P201, P202, P203, P204, P205, P206, P207, P208 DISABLED. |
| 18 | Scarsdale Water Treatment Plant<br>Manipulation of Raw Water Pumps: P101 & P102 DISABLED. |
| 8 Sep (Team D) | |
| **19*** | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 OPEN. |
| **20*** | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 CLOSE. |
| **21*** | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 OPEN. |
| **22*** | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 CLOSE. |
| **23** | Scarsdale Water Treatment Plant<br>Exploit of Primary Historian |
| **24** | Scarsdale Water Treatment Plant<br>Manipulation of Raw Water Pumps: P101 & P102 ON. |
| **25** | Scarsdale Water Treatment Plant<br>Manipulation of motorised valve: MV101 CLOSE. |
| **26** | Scarsdale Water Treatment Plant<br>Manipulation of Raw Water Pumps: P101 & P102 OFF.<br>Spoof value of Raw Water Level Meter: LIT101.<br>Manipulation of motorised valve: MV101 CLOSE. |
| **27** | Scarsdale Water Treatment Plant<br>Ransomware the Historian Data. |

## 13.2. Performance of FLBI and BTVs

Table  shows the attacks detected by each IHL ADM and BTVs. A cell marked "X" indicates that the attack was detected. Table  summarises the performances of the ADMs and BTVs.

*Table 2: Detection of attacks by ADMs and BTVs.*

| Attack No. | FLBI | BTV01 | BTV02 | BTV03 |
|---|---|---|---|---|
| **1** | | X | X | |
| **2** | | X | X | X |
| **3** | | X | X | X |
| **4** | | X | X | |
| **5** | | X | X | |
| **6** | | X | X | |
| **7** | | X | X | |
| **8** | | X | X | |
| **9** | | X | X | |
| **10** | X | X | X | |
| **11** | | X | X | |
| **12** | | X | X | |
| **13** | | X | | |
| **14** | | X | | |
| **15** | | X | | X |
| **16** | | X | X | X |
| **17** | | X | | X |
| **18** | | X | | X |
| **19** | X | | X | |
| **20** | | | X | |
| **21** | | | X | |
| **22** | | | X | |
| **23** | X | | | |
| **24** | | | | X |
| **25** | | | | |
| **26** | | | | |
| **27** | | | | |

*Table 3: Performance of ADMs and BTVs.*

| Detector | Total Attacks | Total Yes | Total No | % Detected |
|---|---|---|---|---|
| **FLBI** | 27 | 3 | 24 | 11.11% |
| **BTV01** | 27 | 18 | 9 | 66.67% |
| **BTV02** | 27 | 17 | 10 | 62.96% |
| **BTV03** | 27 | 7 | 20 | 25.93% |

## 13.3. Analysis of Performance

From Table , among the BTVs, BTV01 performed the best. One attack to note is Attack No. 23. This attack brought the Historian down; only FLBI was able to detect this. As described in Section 12.3, FLBI is a blockchain-based ADM that compared the values in the PLC and the Historian. As such, it was able to detect that the Historian was down while the other detectors could not.

Attack 27 was specifically investigated. This was a ransomware attack that encrypted the historian files and values which was not detected by any of the BTVs. Even though there has been a spate of ransomware attacks in real Industrial Control Systems, this attack still went undetectable. In the recent Colonial Pipeline ransomware attack[3], the company was forced to shut down its fuel distribution operation and freeze IT systems. Therefore, detection of a ransomware attack is crucial to the future of ICS detectors.

## 14. Summary

This year, CISS had a total of 10 Red Teams in the finals and six Blue Teams Vendors and six IHL ADMs who took part in this event. The Red Teams had a unique opportunity to attack a much larger realistic network of process plants to cause process anomalies. The attacks allowed us to understand composite Tactics, Techniques and Procedures (TTP) that can be used for enhanced Operation Security (OpSec).

A quick observation was that although most teams had managed to launch several attacks, the lack of knowledge on the plant's state and processes greatly affected their effectiveness and situation awareness. Most teams were adept at first-order attacks such as closing motorised valves, turning on and off pumps. However, they also did not take time to understand what the current state of the plant was. Hence, certain objectives that required waiting time, such as suspending the backwash process in Stage 3 or resetting the system before the next attack, were not completed successfully.

**<End of document>**

[3] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/