iTrust
Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Critical Infrastructure Showdown 2020-Online

[CISS2020-OL]

Results and Preliminary Analysis

Tuesday Aug 11, 2020

Agenda

- Welcome
- Attack data
- Alarm data
- Feedback
- Red team performance

Members of RED teams

Members of BLUE teams

Members of GREEN teams

Judges

National Research Foundation and MINDEF

Thank You

CISS2020-OL Team

Andres Murilo

Beebi Siti Salimah Binte Liyakkathali

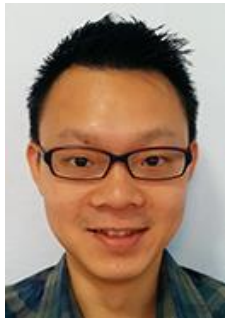
Francisco Furtado

Dr. Gauthama Raman Mani Iyer Ramani

Ian Teo

Ivan Lee

John Henry CASTELLANOS



Mark Goh

Angie Ng

Muhammad Syuqri Bin Johanna

Siddhant Shrivastava

Sridhar Adepu

Surabhi Athalye

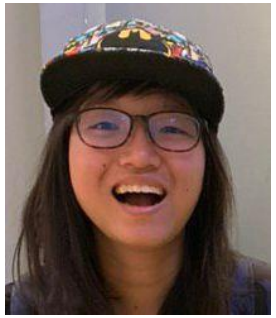
Priscilla Pang

Hor Miao Yun

Yuqi Chen

CISS2020-OL Student Support Team

Attack Logger



Lau Yu Hui

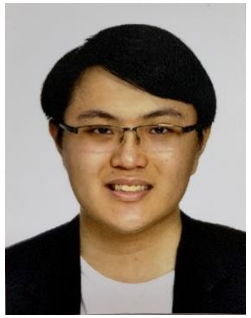
Twin Virtualization

Lim Yang Zhi

Superdetector

Madhumitha Balaji

Zycron



Ng Jo-shen

AR/VR for ICS

Tan Li Yuan

Infrastructure: Hardware

Secure Water Treatment Plant [SWaT]

Zycron Cyber City

- 8 servers, CCTV system and network printer
- 150 virtual, firewall, CCTV, printers, switches
- user terminals("accounts"), DNS server, DHCP server, email server, FTP server, billing server, intranet server, versioning server, etc
- Roughly 10,000 IP
- ICS Honeypots

Infrastructure: Software

PlantViz: SWaT Visualization

PlantIO: Hosts anomaly detectors

Attack logger

Alert logger

Player and data analyzer

Digital Twin for SWaT

Infrastructure: Detectors

AEGIS

AICrit

Attester

DAD

HybMon

Stef-Net

Stef-Phy

Superdetector

Commercial: EBT01--EBT05

Participation

Role	Count
Attackers	84
Defenders	32
Judges	4
iTrust	18
Total	**138**

TEAMS	Count
RED	17
BLUE	15

Data

IT Data [pcap]: 939.3GB in 5777 files

OT Data: 113 MB in 18 Excel files each with 63 features

Data Duration:

Normal and attack mode: ~88 hours

Attack mode (included in above) : ~73 hours

For the advancement of Science and Engineering of Critical Infrastructure Defense

In accordance with iTrust policy,

all data,

suitably anonymised,

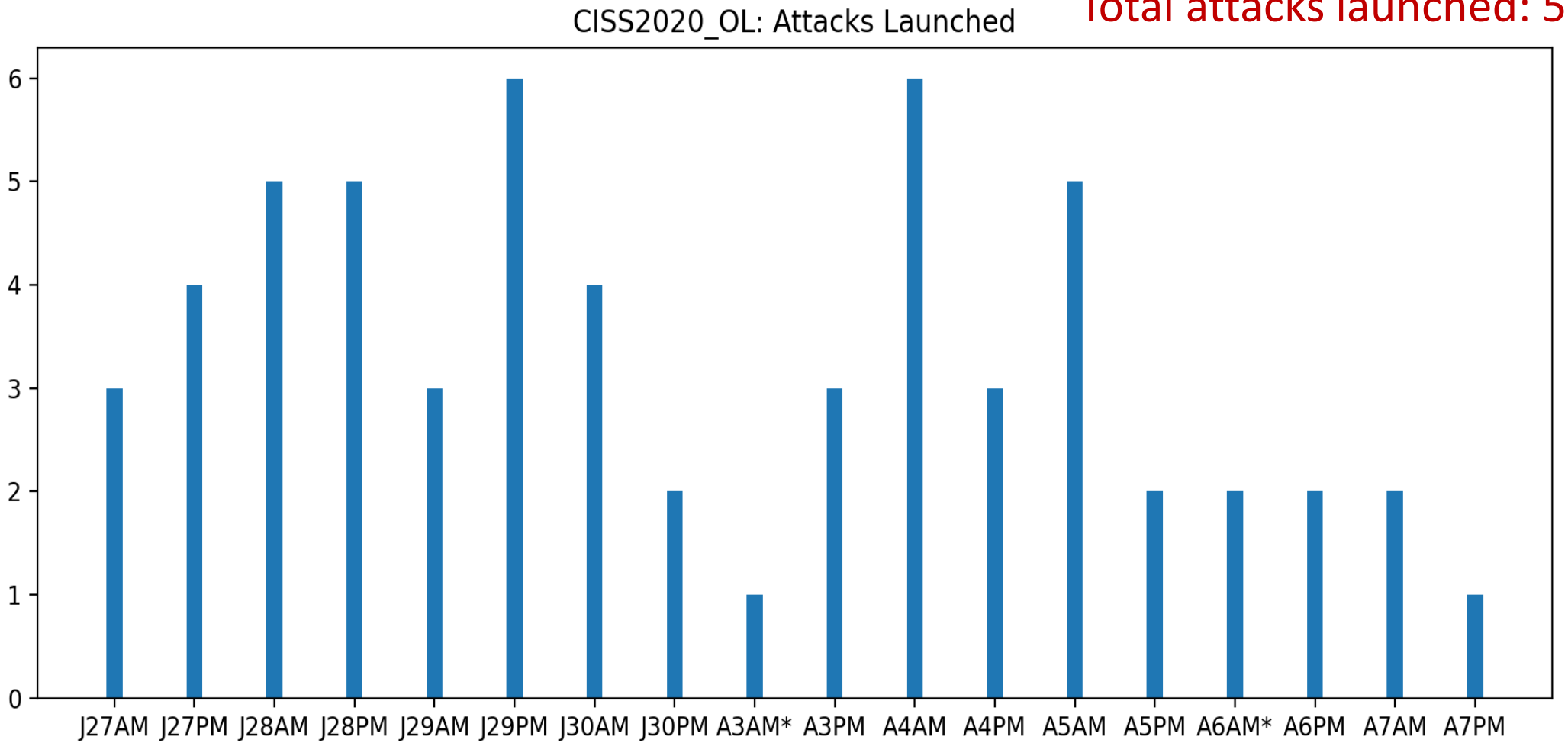
will be made public soon after all blue

teams have completed and reported to

iTrust their data analyses.

Attacks Launched

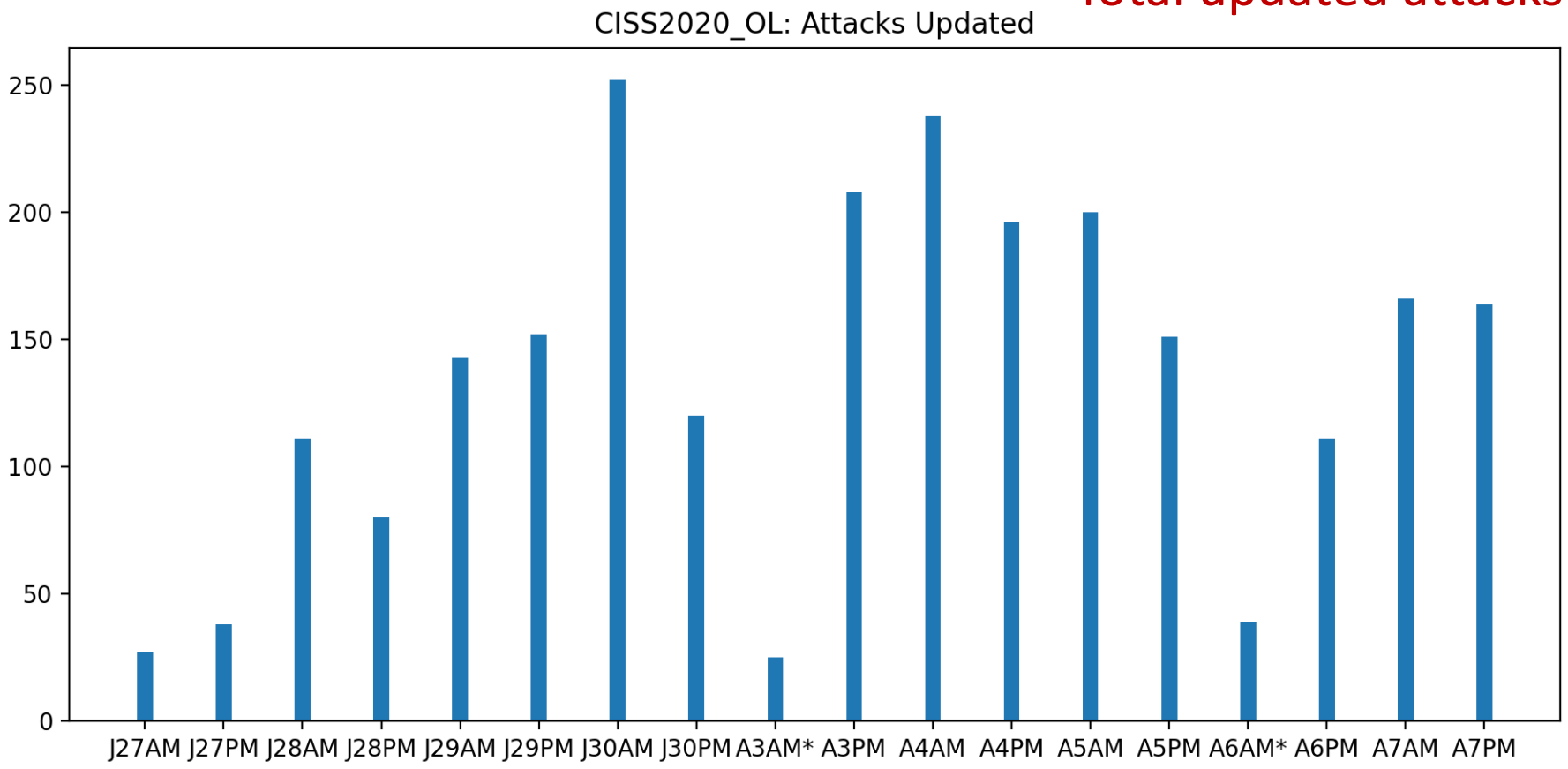
Total attacks launched: 59



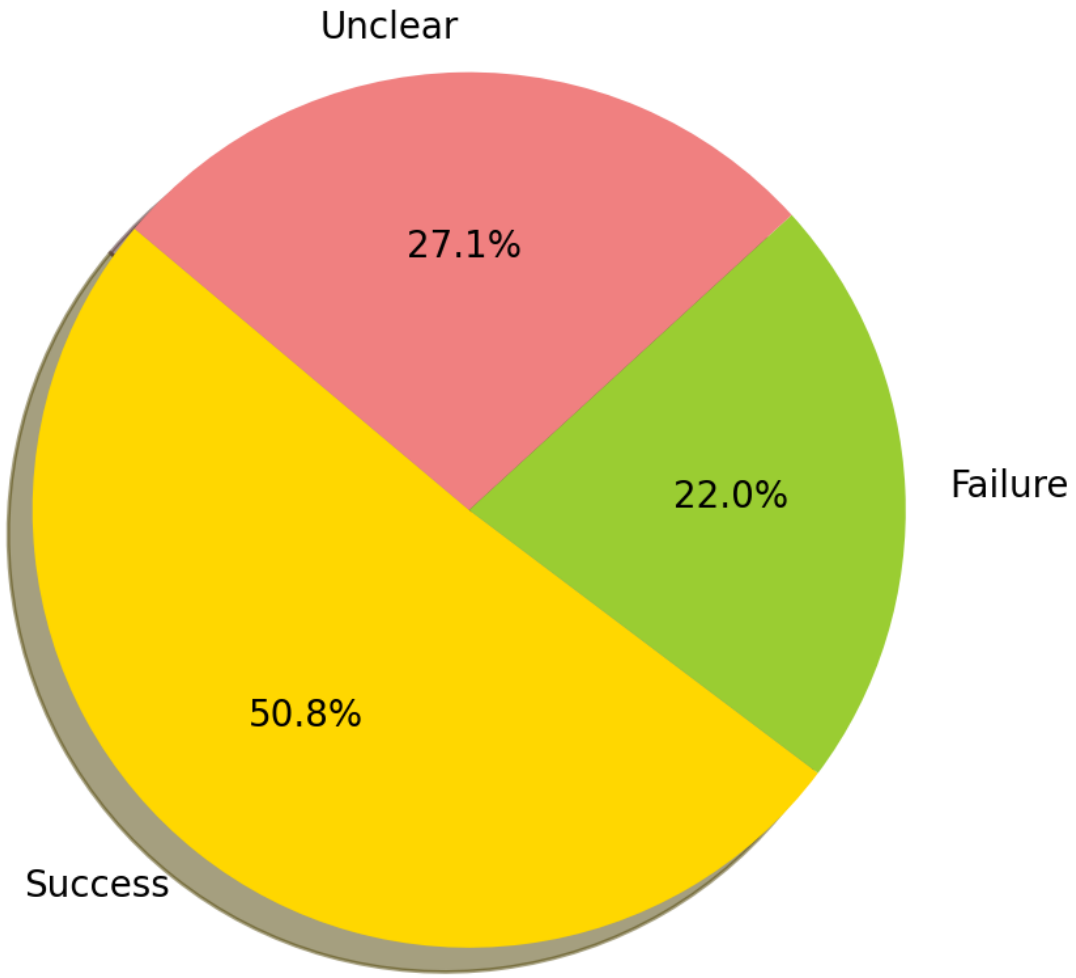
* iTrust RED Team

Attacks Updated

Total updated attacks: 2,480



Attack Success and Failure



Sample of Attacks Launched

exploitdb Rockwell FactoryTalk View

Constant

Man-In-The-Middle

Denial-of-Service (DOS)

Gradual-Bias

Chatter

eternal blue

Password Attack

Stopping plant control

Devastating Impact: Service disruption

PLC1 stopped by moving it to “Test” mode

This resulted in stopping the plant.

It took plant operators and engineers about 30 minutes to discover and fix the problem and bring the plant back into operation; control logic had to be reloaded into the PLC.

Devastating Impact: Plant Flooding

Control taken over PLC

Water level in tank T101 keeps rising.

Inlet valve MV101 closed manually.

Water level continues to rise as there is another inflow from stage 6 of the plant.

Panic sets in and multiple engineers join hands to stop the flooding; water did not overflow the tank..

As a precautionary measure, electric power to the plant shut off to avoid short circuiting the PLC racks. About 40 minutes to get the plant back up.

Alarms and Alerts

Data is sent to each detector once every second.

Alarms generated by each detector are recorded.

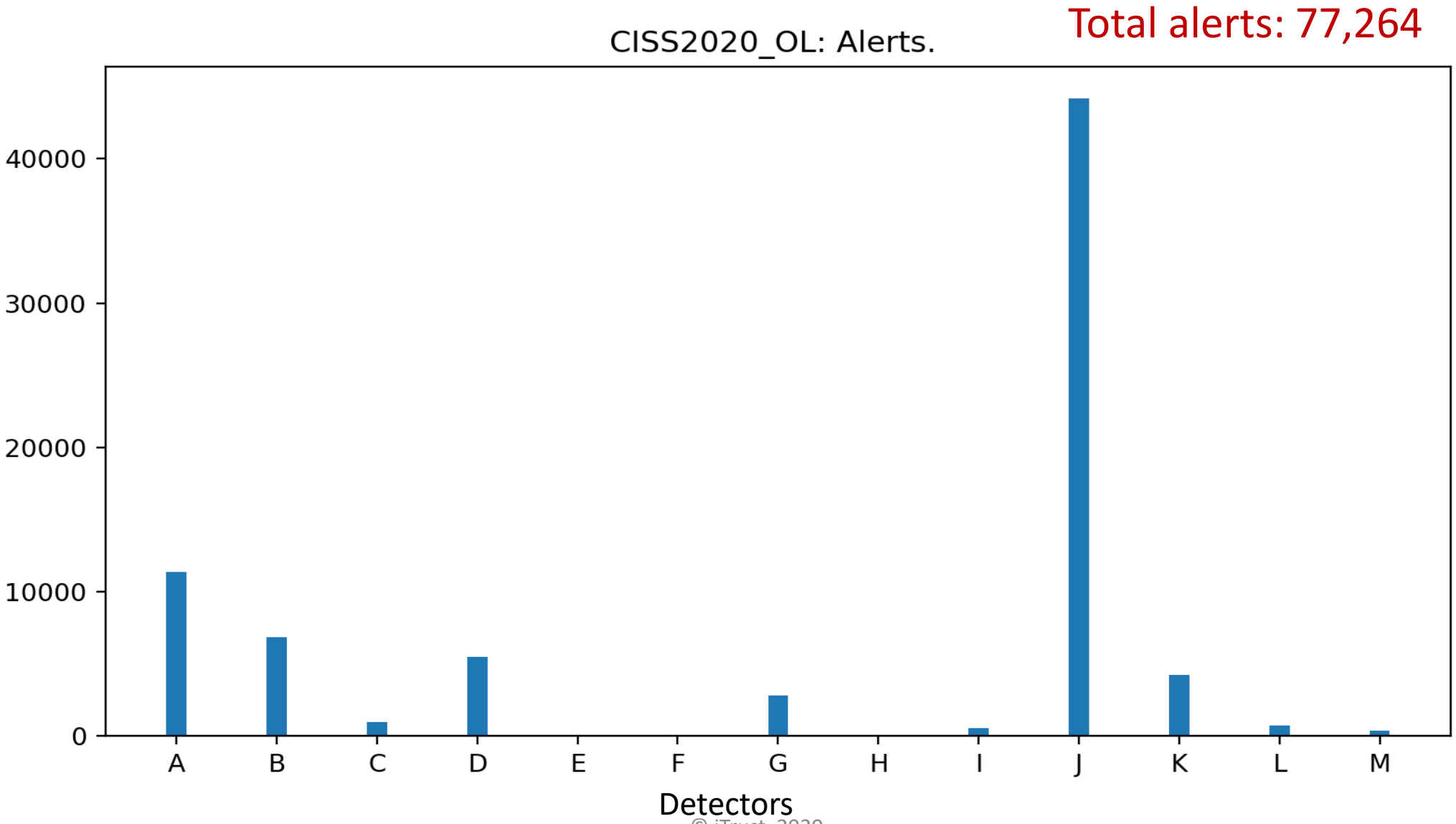
Alarms reported here have not been analyzed. Thus, we do not know yet whether an alarm is a True or a False positive.

A sequence of identical alarms is considered as one alert.

Thus, the number of alarms generated is much greater than the number of alerts reported here.

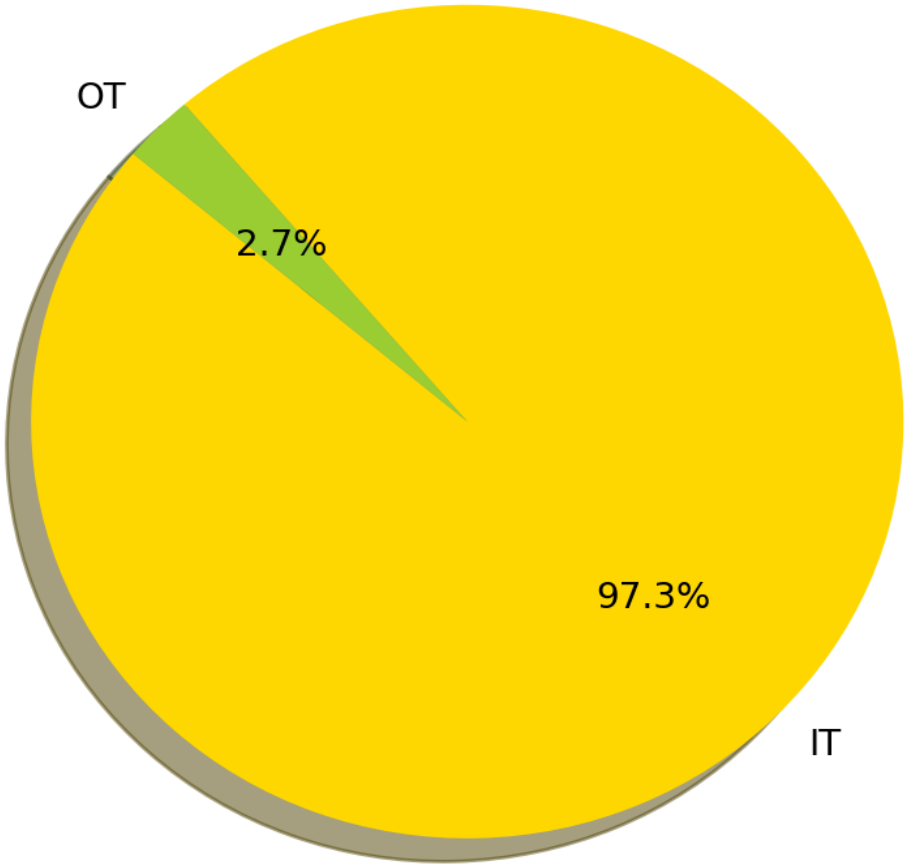
Alerts

Total alerts: 77,264



Attack Modes

Mode	Meaning
IT	Network attack in an attempt to get to SWaT; exploration
OT	Success in getting into the plant; attempting to manipulate plant state



Attack Targets

Unspecified
Level
Valves
Plant
Pumps
SCADA
PLCs
All
Historian
MV101
FIT101
DPIT301
Conductivity

Most common targets:
Unspecified
Level
Pumps
PLCs

Notable Cyber-Physical Attacks

Attack C

- Managed to affect **every major operational process** in SWaT and were nice enough to revert their attacks to not cause plant damage.
- **Affected water quality** in chemical dosing processes by switching on pumps.
- Used **varied** attack vectors (HMI, PyLogix).
- Increased the **alkanility** of water by affecting NaOCL dosing in stage 3.
- **Multi-stage attack by triggering consequent flooding** in stage 1.

Attack B

The team displayed a deep understanding of the plant's OT and IT systems at the process level.

Two attack vectors were used to disrupt the stage 1 process – **HMI and PyLogix**.

Switched on the pump P101 via PyComm while forcing Motorized Valve MV101 to stay closed thereby building **catastrophic amounts of water pressure in the pipes that could potentially burst them**.

Spoofed Flow Meter readings in conjunction to satisfy the PLC's safety conditions.

Attack-A

- Established persistent access on SCADA system via RDP.
- Modified the Programmable Logic Controllers' code using Ladder Logic and Structured Text to **insert a malicious tag** in stage 1.
- The tag modified the level sensor's values and motorized valve's values to cause **flooding if unmonitored**.
- The PLC tags were also read and modified via PyComm as a separate attack vector.
- Effectively equivalent to a **Man-in-the-Middle attack** where operator sees a safe value on the HMI while the PLC uses tampered values.

Top Performers-3

1st place: KopiTiam

2nd place: KPMG

3rd place: JYVSECTEC (JAMK)

Planning for CISS2021 has begun!

We need your input to make the next CISS even better!

Click here to provide your feedback.

Thank You!

Looking Forward CISS2021-OL