The Fourth International

Critical Infrastructure Security
Showdown - Online
2020

Briefing for Blue Teams

22 June 2020, 9 – 11am

SUTD, LT3 & Zoom

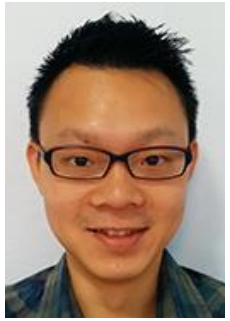
Mark Goh, Francisco Furtado, Muhammad Syuqri Bin Johanna

Agenda

- Introduction to CISS2020-OL Team
- Objectives of CISS2020-OL
- Schedule
- Blue Team infrastructure
- Alert logging:
  - Integration with PEPR
  - Alert Logger
- Q&A

Introduction to CISS2020-OL Team

Event oversight and management



Mark Goh

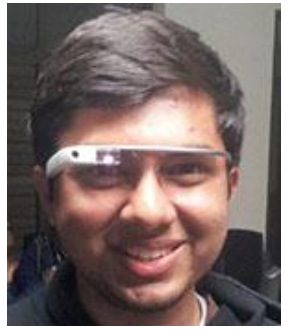
Aditya Mathur

Beebi Siti Salimah Binte Liyakkathali

Technical support

Francisco Furtado

Ivan Lee



Siddhant Shrivastava

Ian Teo

Muhammad Syuqri Bin Johanna

Introduction to CISS2020-OL Team

Tools

Surabhi Athalye

Ivan Lee

Aditya Mathur

Gauthama Raman Mani Iyer Ramani

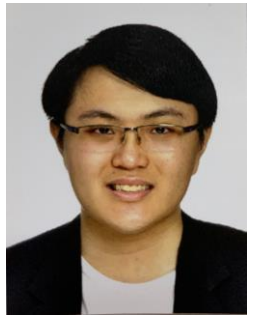
Siddhant Shrivastava

Student interns

Madhumitha Balaji

Lau Yu Hui

Lim Yang Zhi



Ng Jo-shen

Tan Li Yuan

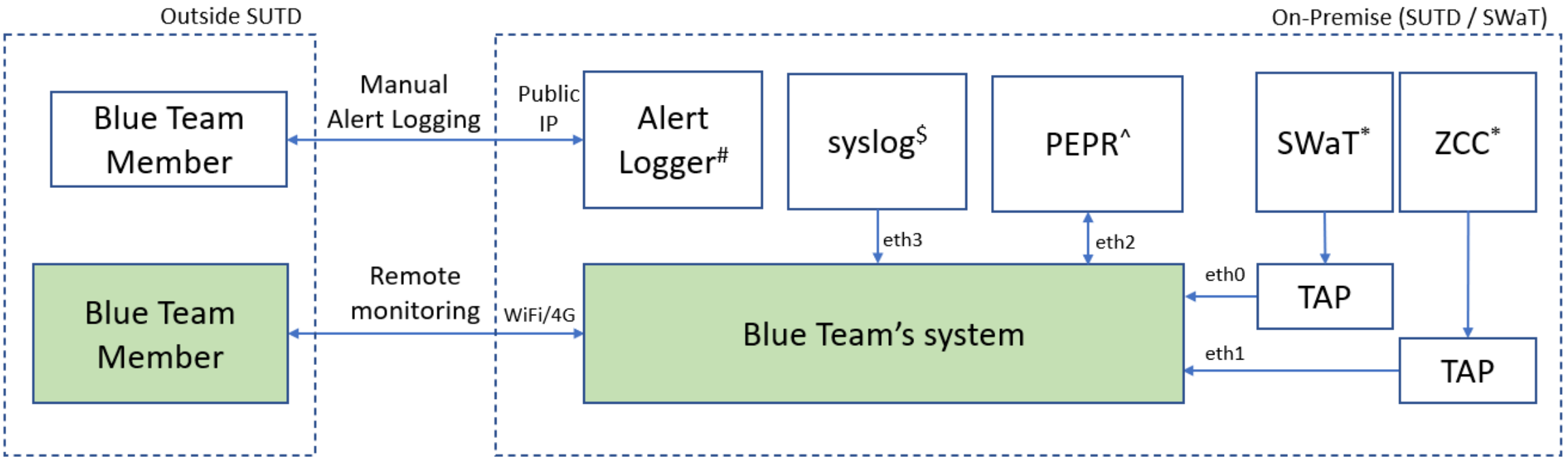
Objectives of CISS2020-OL

- Validate and assess the effectiveness of technologies developed by researchers associated with iTrust
- Develop capabilities for defending critical infrastructure under emergency situations such as cyber-attacks
- Understand composite Tactics, Techniques and Procedures (TTPs) for enhanced Operation Security

Schedule

Phase I [May 4 - 29, 2020]	Participant selection (red & **blue teams**, observers)
Phase II [June 22 - July 3, 2020] • **Phase II-A [June 22]** • **Phase II-B [June 29]** • **Phase II-C [TBC]**	Participant familiarisation (red & **blue teams**) **Blue team briefing** Red team briefing Judge briefing
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

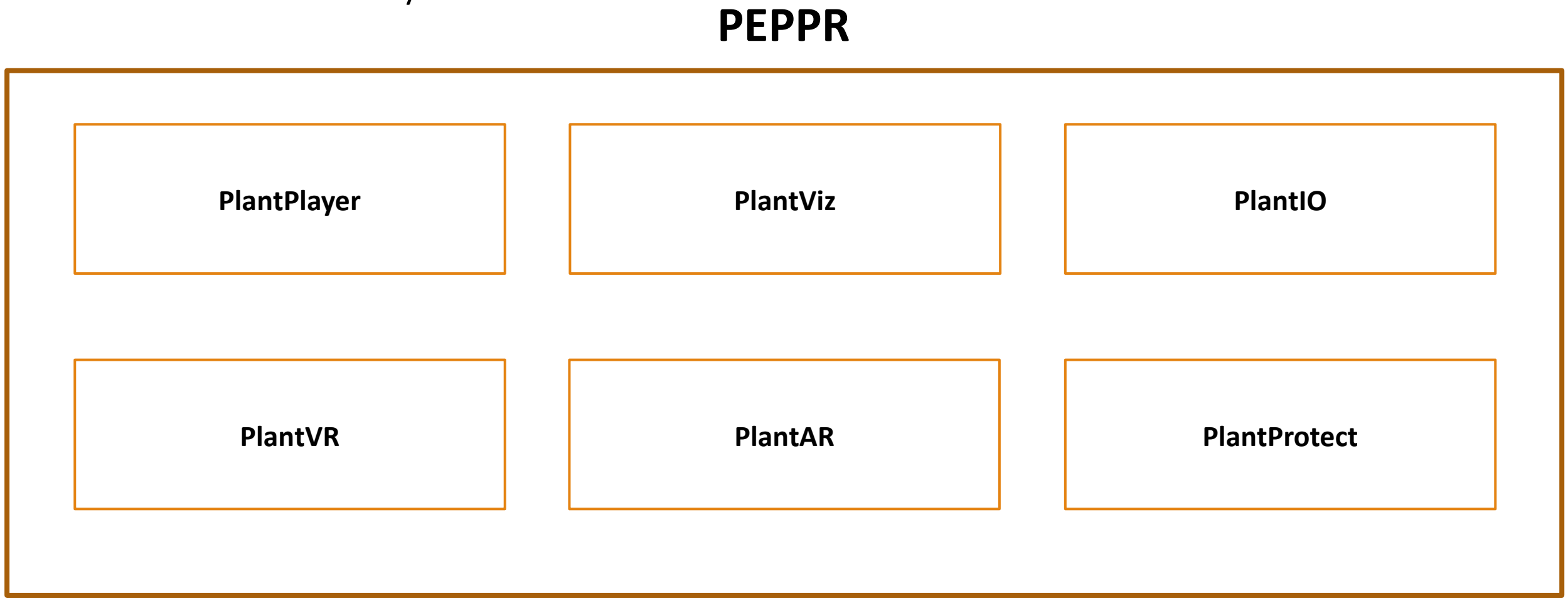
Infrastructure for Blue Teams



* - Data provided is live network packets from SPAN ports
^ - Data provided is a dictionary of the OT variables, key value pairs
$ - Data provided is syslog from SCADA and HMI only. To be confirmed
# - Expects a multi-part message consisting of a string topic and a JSON data part, wrapped in ZeroMQ protocol, It can then display the alert in a visualised format.

Integration with PEPPR

PEPPR: Collection of tools (PlantPlayer (PP), PlantViz (PV), PlantVR (VR), PlantProtect(Pro), PlantAR (AR) and PlantIO (PI)) that allows playback of historical data to enable blue teams to test their own detection systems



Purpose

- To send alerts to PlantViz for immediate visualisation
- To send alerts to PlantIO for logging and saving of data
- Saved data can be used for post-event analysis

Requirements

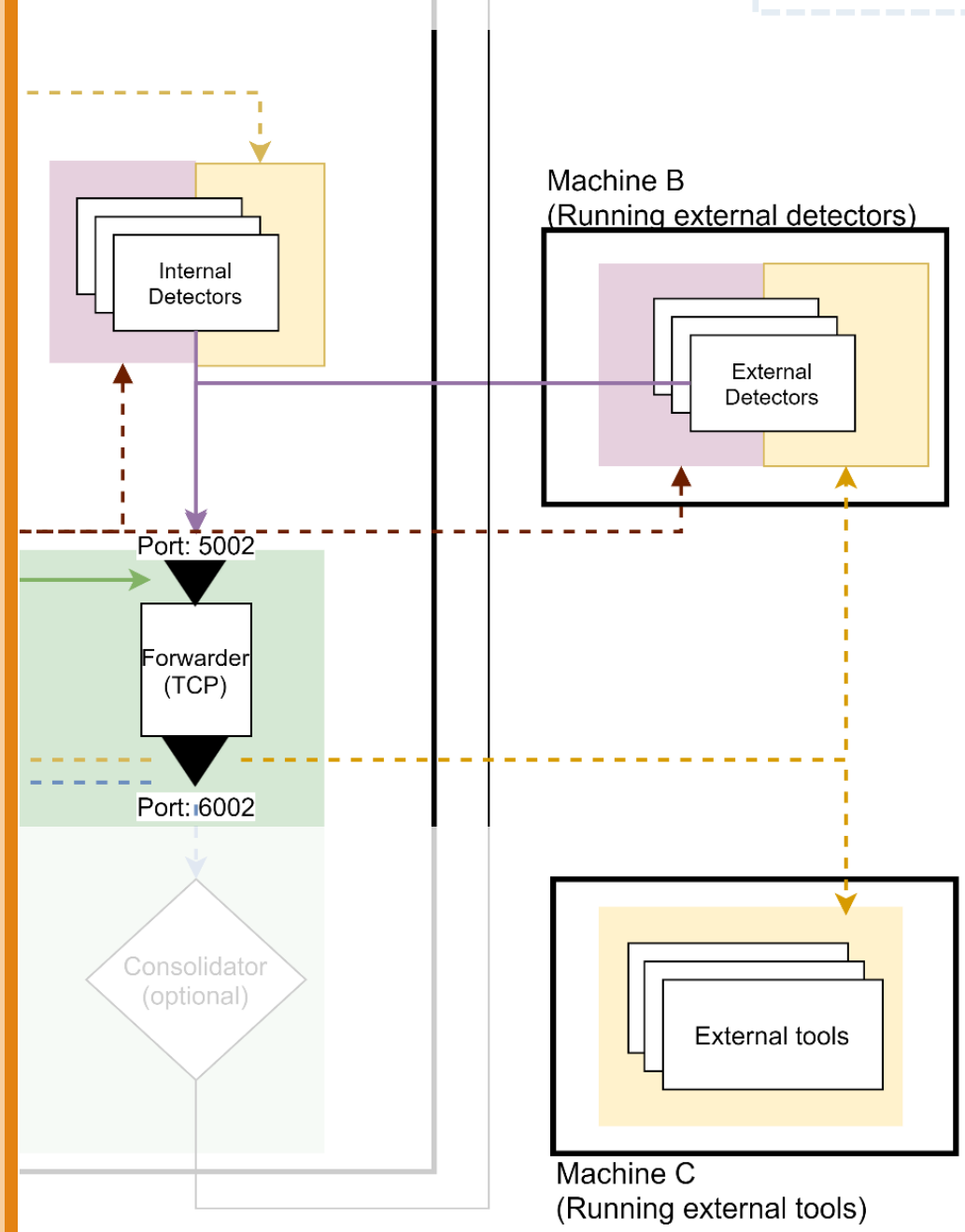
- Manual configuration on detectors' end
- Usage of the ZeroMQ protocol to send alert

Additional Requirements

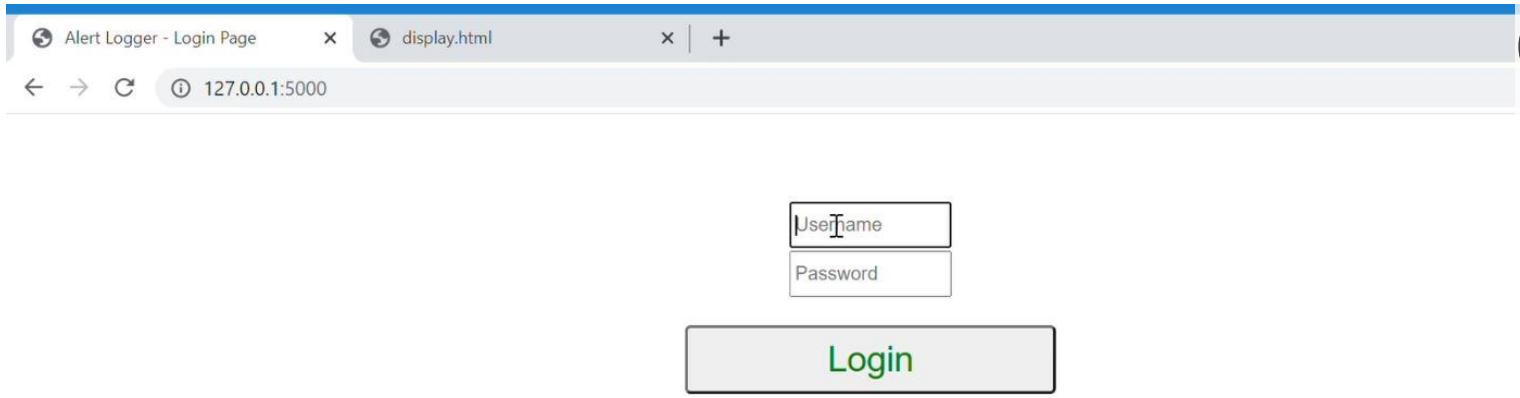
- Sending of two-part message with the ZMQ protocol consisting of:
  - First part – type String
  - Second part – type JSON
  - Formats will be specified upon confirmation of integration
- Send to a server in SWaT at port 5002

External Detectors

- External detectors can send their alerts to the Forwarder so that PlantViz and PlantIO can receive it
- Forwarder details:
  - Located at port 5002
  - Connected and configured via ZMQ

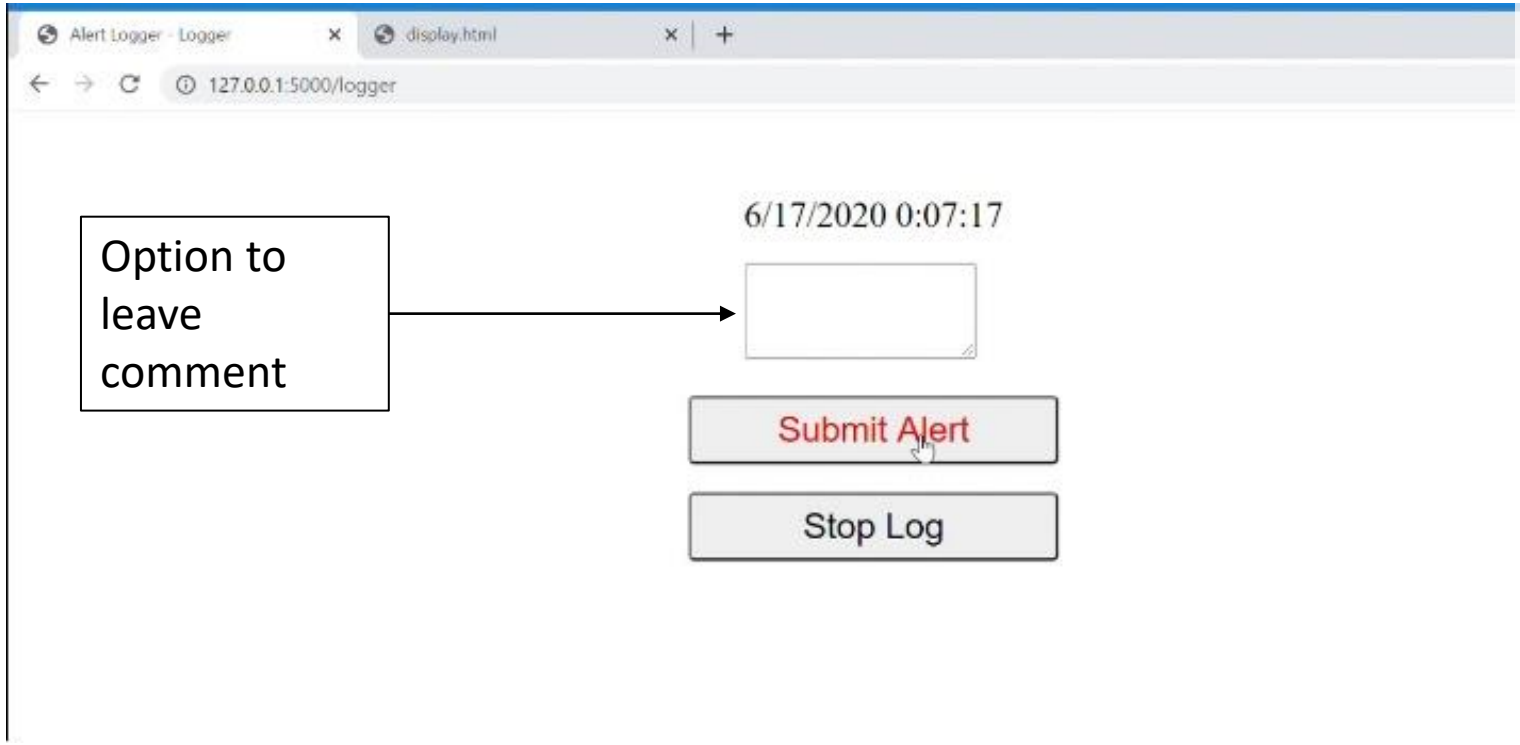


Alert Logger



Operation

- Each blue team will be given a username and password to login
- Important to note:
- Click “Submit Alert” button as soon as your system informs you of an alert
- Time-stamped
- Only alerts logged using logger will be used for analysis (detection rate + false positives)
- Delays (time between attack launched and alert logged) will be reported
- Logging alerts on attacks on SWaT only



Passive Monitoring, Active Logging

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 3.2.3, **there shall be no effort made by the blue teams to prevent, halt or thwart any attacks launched by the red teams.**

Thank You
Q&A