1. **How many power sockets are provided to blue teams?**

   We can provide up to 5; if more is required, please let us know.

2. **Is rack or table space provided for blue teams' equipment?**

   Only table space is provided. Please note that no Blue Teams will be allowed in the testbed premises during the CyberFire phase.

3. **Are monitors, keyboard, mouse, PC, VM etc. provided by iTrust?**

   No, please bring your own hardware to be set up in SWaT; your hardware should also enable you to set up/run your own virtualisation if needed.

4. **Is NTP server provided by iTrust?**

   No.

5. **Can blue teams bring their own 4G router to, for example, transmit data?**

   Yes.

6. **What if we are unable to complete installation during our allotted slot?**

   You can book another slot using the online poll website. Each slot is 2 hours, and each blue team can book up to 3 slots.

7. **Will blue teams be given time to perform baselining of SWaT? Is time taken to achieve baselining a factor in scoring blue teams?**

   Baselining is available to blue teams, please let us know how long you need SWaT to be running. We are not scoring blue teams per se i.e. no scores will be given, and the time taken to achieve baselining is not part of our assessment of blue team's performance in terms of attack detection rates, delays (time between an attack was launch and time reported) and number of false positives.

8. **Will iTrust be assigning IP addresses to blue teams' systems?**

   As blue teams' systems are receiving data from SPAN port, there is no need to assign IP address.

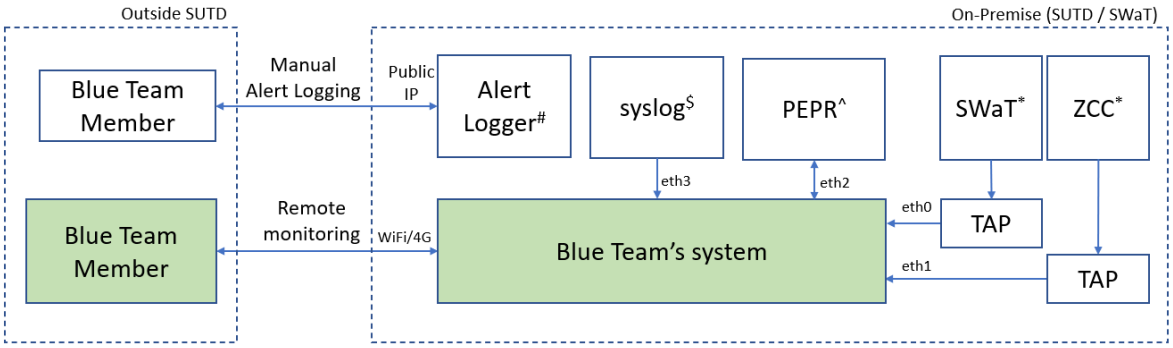
9. **Are Blue Teams expected to have their systems switched on during the entire two weeks?**

Yes they must be switched on during the CyberFire slots; during system reset and other periods, Blue Teams can turn them off if needed.

10. Must blue teams decommission their systems at SWaT immediately after the CyberFire exercise on 6 August?

No, they can do so the following week.

11. Referring to the diagram below (Francisco to update diagram):



* - Data provided is live network packets from SPAN ports, throughput of 1mbps each, bandwidth of 1Gbps
^ - Data provided is a dictionary of the OT variables, key value pairs. If integrated, **auto alert logging** is enabled.
$ - Data provided is syslog from SCADA and HMI only. To be confirmed.
# - Simple Webapp for manual alert logging. To be confirmed if it is internet facing

a. What does "Blue team's system" mean? Is it a virtualised box or a physical hardware that the blue team will need to install?

It is the blue team's hardware and/or software that is receiving data from SWaT and Zycron Cyber City through the TAP switch. As such the blue team system is the one that decides if SWaT is under attack or behaving normally. The blue team then informs of the alert either through PEPPR automatically or through the Alert Logger manually.

b. Using Alert Logger, can multiple members from the same Blue Team enter logs at the same time?

Yes. Each member from the same Blue Team will be given a unique login to the Alert Logger. However, the maximum number of logins provided to each Blue Team is 4. Please let us know how many accounts you require.

c. Does connection to syslog, Alert Logger and PEPPR require dedicated/individual physical connection?

PEPPR: Physical connection and same subnet as SWaT

Alert Logger: while it shares same connection with PEPPR, blue teams do not require a physical connection to Alert Logger; we are currently trying to make it internet facing through a web browser

Syslog: currently it does not share the same connection with PEPPR and Alert Logger, but we are trying to achieve that

d. Are syslog, Alert Logger and PEPPR in the same subnet?

Currently they are not, but we are trying to achieve that.

e. Can we automate the process of sending alerts from the Blue Team's system to the Alert Logger?

Two options are provided to blue teams to log alerts, and blue teams need to only choose one option. One is through PEPPR, the other is through a manual system called Alert Logger (internet facing). If the blue team opts for its system to be integrated with PEPPR then the alert logging process via PEPPR can be done automatically. Do note that messages sent from the blue team's system to PEPPR has to be done through the ZeroMQ protocol specified in a multi-part message format (starts with a string and ends with JSON format.) For those wishing to use PEPPR, Syuqri will send a manual for integration and an example of the nature of the data to be expected from PEPPR.

f. Data from eth0 + eth1 is piped via a 1Gbps RJ45 connection; does it mean there are two ethernet connections coming from the TAP switch? What is the expected sustained traffic from the TAP switch?

Two ethernet cables (one from IT (ZCC) and one from OT (SWaT)) will be provided for the connections. Expected sustained traffic is 4Gb per hour (1.11 mbps) per eth

g. How many SPAN ports are there?

2 SPAN ports; one from OT (SWaT) and one from IT (ZCC)

12. Can you provide a list of assets in SWaT used during CyberFire?

List of equipment in SWaT can be downloaded here.

13. Is there a cap on the number of blue team members doing remote monitoring?

No cap. However, the maximum number of logins provided to each blue team is 4.