1. **In the Crossed Swords exercise, the SWaT testbed used a certain protocol. Is this protocol remained unchanged?**

   Yes, it remains unchanged.

2. **By "dataset" are you referring the historical data from the sensors and client/server machine?**

   Yes, it refers to the data coming live from plant and going into historian before it is being retrieved.

3. **What is the goal of picking targets in advance?**

   Target selection is posed as an additional challenge to red teams, as it gives iTrust the opportunity to learn how red teams analyse and identify the dataset.

4. **Are we expecting the digital twin (DT) to react the same as SWaT?**
   DT is designed to behave similar to, but not exactly the same, as SWaT. All controls in DT follow the same algorithms as those used in SWaT.

5. **How many days do we have to prepare these attacks? How often can we access SWaT for testing?**

   You can start preparing your attacks now. However, you will only be able to access SWaT during the 4 hours CyberFire phase. This is where you can design, test and launch your attacks.

6. **What is considered as a successful attack?**

   A successful attack is where the attack target that you selected e.g., a running pump, has been manipulated e.g., by causing it to stop.

7. **When will we know our objectives, in order to prepare our attacks? Do we get more points if our attacks are undetected?**

   Yes, refer to para 3.4.4 of the guidelines for the scoring mechanism and formulae.

8. **What do LIT, AIT, FIT etc. mean?**

You can download a copy of the SWaT's technical details here. This document contains details of SWaT including process diagrams and components. Details of components, e.g., pump characteristics, are also in this document. You may use this document to design attacks.

9. Are there any attacks that are not allowed?

Yes. For example, if you are able to access the detectors, please do not disable them! There is also a list of blacklisted attack targets found in the footnote of para 3.4.4 of the guidelines. More will be added to this list in the next version release of the guidelines.

10. Will our VMs will have access to internet? Will we be able to push tools onto those machines before the attack?

Yes, each red team will be given internet access to their VMs 30 mins before their CyberFire session begins. Once the CyberFire session begins the internet access will be cut off. You will also be able to push tools to your VM within this 30 mins.

11. During our attack, can we still push tools to the VM?

Yes, but only those that do not require internet connection since there will not be internet connection once CyberFire starts.

12. If we want to use a custom VM, how would we go about passing it to you?

Please email the download link of the VM to ian_teo@sutd.edu.sg, we will install and invite you to test it.

13. When do we need to pass you the custom VM?

As soon as it is ready, minimally 3 working days before your CyberFire slot, but preferably one week before.

14. Does the VM provided come with the necessary tools e.g., Python 2 or 3?

All VMs come with Kali Linux, Windows 10, and Python 2 and 3. Windows 10 will come with basic Commando framework installed. Red team members are required to install their respective tool packages in Commando for Windows 10.

15. **For Kali Linux version, is it the most recent rolling release or some specific older release?**

    It will be the latest version, but if you need a specific version, please provide a copy of that version to us to be installed.

16. **The diagram states that there is Zoom/Skype call with screen recording. Does this mean that the screen of the red team members will be recorded?**

    Yes, during the 4 hours of CyberFire we require all red teams to share the screens that show the state and progress of their attacks (e.g. running attack scripts), but we do not require them to show their faces to the camera. All audio and video will be recorded for post-event analysis and reporting, but we will not share the audio and video recordings with anyone without your permission.

17. **Will the judges inform whether the attack is successful?**

    Yes.

18. **Do findings include the enumeration of the Zycron corporate network? i.e. do those need to be reported too?**

    Yes, we will log all actions taken by the red team.

19. **Are the data points in the dataset used during target selection analogue or digital?**

    They are all in digital format.

20. **Do we have to let you know the team members' details like name, affiliation etc. once the team is in top 3?**

    Not necessary, but for those who asked to remain anonymous and are placed in top 3, please let us know if you still wish to remain anonymous or whether we can announce your team's country. If you like to receive a certificate of participation, please let us have your team members' names, organisation and mailing address so that we can send you a copy of the certificate. We respect the privacy of all participants.