IoT Cyber Ranges

I am writing a master thesis on designing an IoT Cyber Range where IoT hardware device interaction is important. This is part of my Master study in Information security - Digital forensics at Norwegian University of Science and Technology in Gjøvik, Norway.

I have done a literature review on relevant topics. However, the projects are rarely published until some time have passed due to e.g. reviewing. To get a feel of what is going on right now in the research of IoT Cyber Range field and to understand the practical challenges in implementation this questionnaire is distributed to you. Hopefully you will take the time to answer my questions and comment on other aspects that you think is relevant. You have been chosen as recipient because your name is in one of the papers I've read, or you are listed as contact for some relevant projects. If you feel that you are not the correct recipient for these questions, please forward and/or let me know. If you know of others that may contribute to this project, please forward this to them also.
I am also available through other channels, like Teams, Zoom, phone, etc., if You prefer to communicate through a different media. My e-mail address is kebalto@stud.ntnu.no

Current projects

1. Our IoT Cyber Range is

- ◯ Virtual only
- ◯ Physical only
- ◯ Hybrid

2. What smart/IoT environments are supported?

- [ ] Smart cities
- [ ] Smart homes
- [ ] IIoT/Smart industries
- [ ] Smart transportation
- [ ] Smart health
- [ ] Smart grids
- [ ] Annet

3. What is the Cyber range used for?

- [ ] IoT device development
- [ ] IoT penetration testing
- [ ] IRT training
- [ ] Competitions
- [ ] Forensics training
- [ ] Forensics testing
- [ ] Annet

4. What are the functions and interfaces of the Cyber Range?

5. Other comments about current projects

Systems, tools and standards

6. *What systems, tools or standards are you using for orchestration?*

- [ ] OpenStack Heat
- [ ] OpenNebula
- [ ] Self-developed
- [ ] Annet

7. *What systems, tools or standards are you using for management*

- [ ] Kubernetes
- [ ] OpenNebula
- [ ] OpenStack
- [ ] vCenter
- [ ] Self-developed
- [ ] Annet

8. *What systems, tools or standards are you using for scenario definitions?*

- [ ] TOSCA
- [ ] XML
- [ ] YAML
- [ ] JSON
- [ ] Self-developed
- [ ] Annet

9. *What systems, tools or standards are you using for emulations?*

- [ ] Qemu
- [ ] VMWare
- [ ] Virtual Box
- [ ] KVM
- [ ] Xen
- [ ] Mininet
- [ ] Open VSwitch
- [ ] OpenStack
- [ ] Opennebula
- [ ] Self-developed
- [ ] Annet

10. *What systems, tools or standards are you using for simulation?*

- [ ] OMNET++
- [ ] ns2
- [ ] ns3
- [ ] OPNET
- [ ] OpenPLC
- [ ] Self-developed
- [ ] Annet

11. *What systems, tools or standards are you using for monitoring?*

- [ ] ELK
- [ ] Wireshark
- [ ] tcpdump
- [ ] Bro/Zeek
- [ ] snort
- [ ] zabbix
- [ ] sdn controller
- [ ] Self developed
- [ ] Annet

12. *What systems, tools or standards are you using for data representation?*

- [ ] XML
- [ ] Json
- [ ] YAML
- [ ] Self developed
- [ ] Annet

13. *What systems, tools or standards are you using for data creation?*

- [ ] BT3
- [ ] Low Orbit Ion Canon
- [ ] ns3
- [ ] ns2
- [ ] DNP3
- [ ] Self developed
- [ ] Alternativ 7
- [ ] Annet

14. Other comments about systems, tools and standards

Challenges

15. What are the top three functional requirements for IoT Cyber Ranges and security testbeds that differs from general designs?

16. What are the main challenges in cyber range/ security testbed implementations, IoT especially?

17. What are the challenges generating sample benign and malicious data?

18. What needs for IoT usage are not met in your own implementation of cyber range/test bed?

19. How could we address these challenges and functional needs?

20. Other comments about challenges

21. Do you want to receive a copy of the results after the project is finished?

- ◯ Yes
- ◯ No

22. Your e-mail address?

23. Other comments about the questionnaire