Question 2.8 What experiences can be shared on the implementation and operation of Security Operation Centres (SOCs) for EPUs?

Government of India has set up the Indian Computer Emergency Response Team (CERTIn) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats and developed a framework for cyber security.

CERT team identified POSOCO as business criticality organization where they are monitoring the details of servers / traffic. Regularly conducts VAPT on the critical system and inform the respective organizations for such vulnerabilities / phishing / any cyber related attacks.

Moreover, awareness given to the CISO (nodal officers) of all the identified organization and the proper training and awareness of the tools like TeraTeam, WinSCP, HashMyFiles etc and the protocols like IEC 60870-5 -101/104, IEC 62056 series etc.