Securing Critical Infrastructure in Operational Technology (OT) Environments

Scenario Overview:

The OT system controls essential processes, including energy distribution and grid stability in the National Power Grid. Your team, responsible for securing OT infrastructure, has been tasked with identifying secuity risks, and proposing a comprehensive strategy to protect the system from potential threats.

Tasks:

1. **Vulnerability Identification**
    - Identify at least three vulnerabilities commonly found in OT systems (e.g., outdated protocols, lack of network segmentation, limited access controls) and explain how they pose security risks.
2. **Threat Actor Analysis**
    - Research a known OT security incident, such as the Stuxnet or Triton attack, and summarize the methods used by the attackers. Highlight the techniques that would be most relevant to this scenario and the lessons learned.
3. **Impact Analysis**
    - Analyze the potential impact of an OT compromise on the power grid's availability and safety. Consider the effects on public infrastructure, financial implications, and potential downtime.
4. **Policy and Compliance Recommendations**
    - Propose a high-level policy framework for OT security in the energy sector, referencing standards like NERC CIP, IEC 62443, or NIST guidelines. Describe key policy points to ensure compliance and resilience in OT environments.

Deliverable:

Submit a concise report addressing each task with actionable steps, demonstrating an understanding of OT security challenges and the importance of safeguarding critical infrastructure in a ppt format

Create a video explaining your ppt which does not exceed 3 minutes.

Contributors:

The Cybersecurity Centre of Excellence (CCoE) is a glocal hub based in Hyderabad to catalyse innovation, entrepreneurship and capability building in cybersecurity and privacy. It is a joint initiative of the Government of Telangana and DSCI set up to fulfil DSCI's commitment towards creating a safe, secure and trusted cyberspace. https://ccoe.dsci.in/