Industrial Control Systems

Common security practices do apply

PACIFICORP
A MIDAMERICAN ENERGY HOLDINGS COMPANY

Stacy Bresler - CISSP, CISA, CISM
Manager, Corporate Information Security Office

1

First Things First

- I am an active security professional with hands-on security experience in a variety of industries.
- I have been focused on process control security for the past seven years.
- I am a practical person.
- I strongly believe that security is security.
- I learn something new every day.

Security is like a box of ??

- Security principles and practice tend to be the same no matter what they are called - IT security, Physical security, SCADA security, Airline Security and so on.
- Just ‘cause a control system can’t be patched on the same schedule as your corporate network devices doesn’t mean “IT” security doesn’t work.
- Defense in Depth = Defense in Depth , Least Privilege = Least Privilege, Risk = Risk and so on.
- If we practice common security then security compliance is soon to follow.

3

Lewis and Clark Model

- It may be easier to think about what might not work:
  - Corporate environment vulnerability scanning regimes (yes/no/depends?)
  - Corporate patch management programs (yes/no/depends?)
  - Corporate back and recovery solutions (yes/no/depends?)
- THEN...consider the boxes exterior before throwing in the towel.

4

What's working for us...

- My team has found success by leveraging existing tools within the control environments - don't assume the corporate IT way is the only way.
- We have found that there seems to always be a solution in the ***opensource*** community that is flexible enough to be modified for our needs (i.e. SNORT, Argus, TCPDump, Nessus, NMAP, PERL, Linux, etc.)
- Learning each others lexicon makes it easier - speaking to the control system engineers **and** the IT folks!

5