# Cybersecurity Research Needs Vendor Perspective

Bryan Owen PE, OSIsoft LLC

# Beliefs

**Awareness and training are fundamental**

- We need to advance defensive skills

**Cyber defense is a team sport**

- We need collaborative approaches

**Trust is earned**

- We need trust to do great things together

## Motivation (Trust)

AF Tech Horizon's 2010
"In the near to mid-term, developing methods for establishing 'certifiable trust in autonomous systems' is the single greatest technological barrier that must be overcome to obtain the capability advantages that are achievable by increasing use of autonomous systems" (p. 42)

Benjamin A. Knott Ph.D. (Air Force Research Laboratory) https://community.apan.org/wg/afosr/spring_review_2014/m/day_3_2014_-_rtcrtd/132488

# Priority Guidelines

1. **Do No Harm**
2. **Keep the ‘bad guys out’**
3. **Limit damage if they get in**
4. **Hunt for evil**

# Do No Harm – Research Needs

- **Verification and Validation**
  - **Overcome issues of ‘cure is worse than the disease’**
  - **Provable functionality without adverse impact to security controls**
  - **Unexpected changes to ‘baseline’**
- **Representative Test Systems**
  - **How close to real is close enough?**
  - **Requirements for testing beyond N-1 (‘chaos monkey’ for EDS)?**
  - **System of systems interactions**
- **Secure Deployment**
  - **Innovative methods for moving changes to production**
  - **High assurance methods to address deployment drift**
  - **What would it take to reduce level of effort 1000x?**

# Keep the ‘bad guys out’ – Research Needs

- **Prevention is ‘King’**
  - **Tools for EDS operators to identify, optimize, and prioritize prevention barriers**
  - **Research provable methods for emerging SCADA protocols (eg LangSec)**
  - **Research effective/appropriate M2M authentication for EDS ( !=PKI)**
- **Attack surface visibility**
  - **Identify high impact remote exploit paths for a region or by EDS function**
  - **Accelerate development of Cyber Security Data Sheets (EPRI TAM)**
  - **Extend utility of internet based EDS scanning engines (eg Shodan)**

# Limit damage ‘if they get in’ – Research Needs

- **Resilient system architectures for using untrustworthy components**
- **Consider alternatives to ‘fail open’, ‘fail close’, and ‘hold last value’**
- **Study effectiveness of sandbox technology for legacy EDS**
- **Practical study on IDS false positive rate in EDS**

# Hunt for Evil – Research Needs

- **EDS canary based threat hunting methods**
- **Detection methods as EDS protocols ‘go dark’**
- **Is my sensor data fake?**
- **Simulation of deception and delay strategies**
- **Map EDS use of third party libraries to improve supply chain assurance**

# CYBER RESILIENT ENERGY DELIVERY CONSORTIUM


http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

# Content Slide Option #1 – No branding

- This content option does not offer branding.
  - If you want to show branding on content slides, choose:
    - Layout Option 2
    - Layout Option 3.
  - Content goes here
    - And here
      - And here
        - And here