Agenda

➢ Welcome and Introductions

➢ Energy Sector Asset Management (ESAM) Update

➢ Questions, Open Discussion
ESAM CONCEPTUAL ARCHITECTURE

Remote Site

Available Raw Network Traffic

Remote Site
Data Servers
- Passive Sensors
- Passive ICS Asset Discovery Tools

Structured Data

Current Control Systems Management
- Historians
- SCADA servers
- Other Aggregation Devices
*Note: Not all listed devices will be located at each site

Raw Data
(serial-based and other non-routable data)

Control Systems
- PLCs
- RTUs
- Other ICS/SCADA or DCS devices

Note: All cross-boundary network traffic uses secured communication protocols

Enterprise Location

Asset Management Processes
- ICS Asset Management Tools
- Patch Management Tools
- Log Management Tools
- Cybersecurity Event Detection

Asset Data

Events Dashboard

Asset Management Analyst
POOT Asset Management Attributes

➢ **Asset Discovery**: establishment of a full baseline of physical and logical locations of assets

➢ **Asset Identification**: capture of asset attributes, such as manufacturer, model, operating system (OS), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions

➢ **Asset Visibility**: continuous identification of newly connected or disconnected devices, and IP (routable and non-routable) and serial connections to other devices

➢ **Asset Disposition**: the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (to include serial) with other devices

➢ **Alerting Capabilities**: detection of a deviation from the expected operation of assets
ESAM Component List

- OT/ICS specific asset discovery and management tools
- Encrypted communication devices
- Log management/security information and event management (analytics, storage, alerting)
Energy Sector Asset Management (ESAM)

- Call for Collaboration (Federal Register) Released: Monday, 03/26/2018
- Excellent response from tech community
- Stopped Receiving LOIs (Letter of Interest): Friday, 04/20/2018
- All requested capabilities accounted for with overlap
- Currently working with UMD regarding possible deployment at their site
- Multiple sites in consideration and not limited to one
ESAM Tentative Schedule

- Collaborator selection completed: May, 2018
- Build Team Kickoff: June, 2018
- Build Architecture: July, 2018
- Draft ESAM Practice Guide (PG): January, 2019
- Draft ESAM Public Release: March, 2019
Spring 2018

- **OSIsoft:** The 3rd Annual Intelligence and National Security Forum: 05/11/2018, Tysons, VA
  *Presenting NCCoE Energy & Manufacturing Cybersecurity projects to Intelligence Community*

- **Lexington Institute:** Cybersecurity of the Electric Grid Capitol Hill Forum: 06/08/2018, Washington, DC
  *Guest Panelist*
Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide
Jim McCarthy, Senior Security Engineer
Energy Sector Lead
James.McCarthy@nist.gov
301-975-0228
Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.