National Cybersecurity Center of Excellence

Energy Provider Community (EPC) Update

01/30/2018

NIST National Institute of Standards and Technology U.S. Department of Commerce

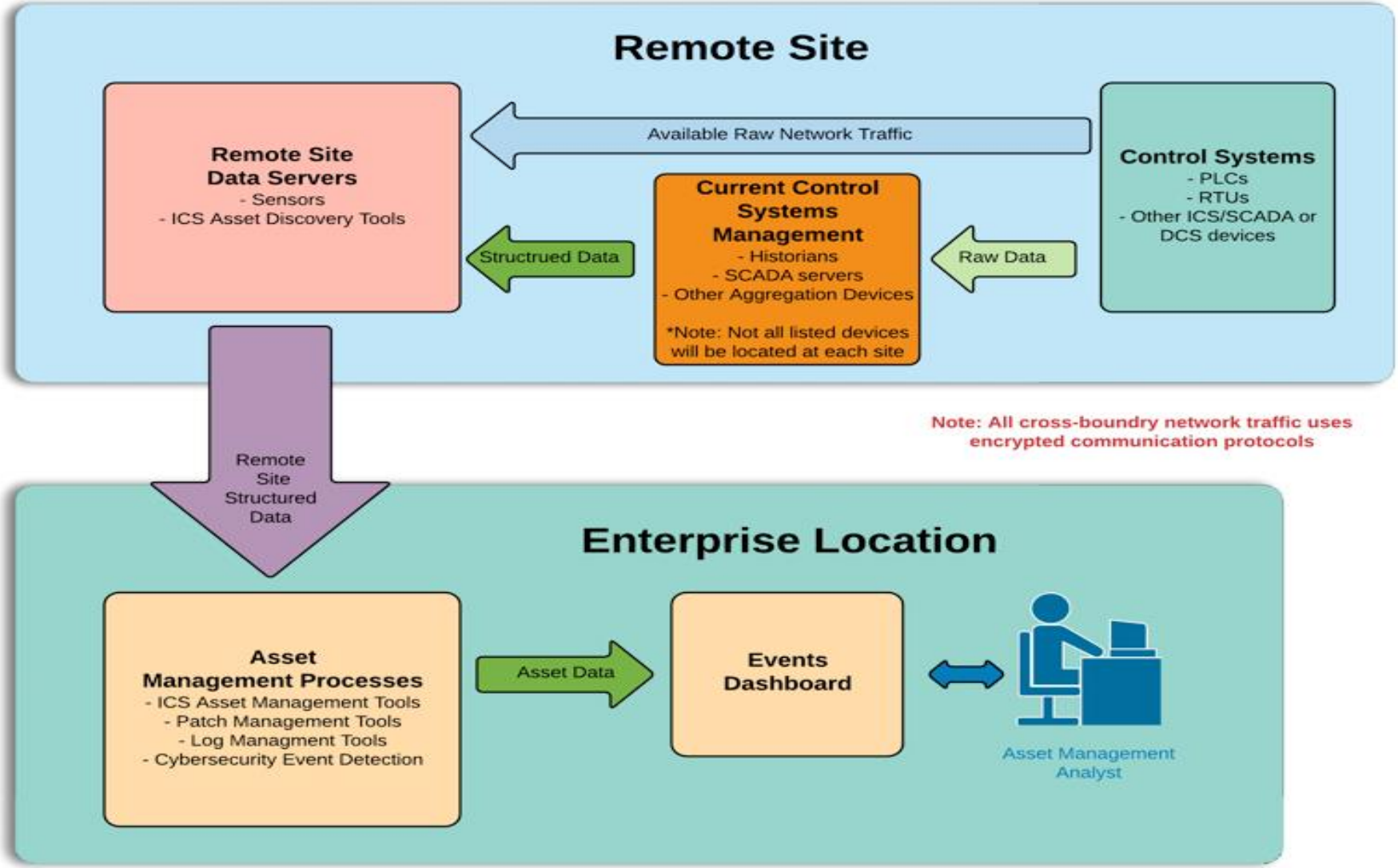
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- Welcome and Introductions
- Energy Sector Asset Management (ESAM)
- Manufacturing Behavioral Anomaly Detection (BAD) Update
- NCCoE Upcoming Activities
- Questions, Open Discussion

- **Energy Sector Asset Management (ESAM)**
  - Draft Project Description (PD) released: 01/16/2018
    - https://nccoe.nist.gov/projects/use-cases/energy-sector/asset-management
  - PD comments due: 02/16/2018
  - Final PD and call for collaboration (FRN): March, 2018
  - Primary Focus on OT / ICS Network assets (including PLCs, HMIs, Eng. Workstations)
  - Interested in collaboration with any utility or lab with numerous OT assets for realistic build

ESAM CONCEPTUAL ARCHITECTURE



- **OT 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, MAC addresses, protocols, patch-level information, and firmware versions
  - **Asset Visibility**: continuous identification of newly connected or disconnected 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 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
  - Patch management tools
  - Encrypted communication devices
  - Log management/security information and event management (analytics, storage, alerting)

- **Manufacturing BAD**
  - **Description**: NIST NCCoE and NIST Engineering Lab (EL) ICS collaborative effort to demonstrate behavioral anomaly detection (BAD) capability for Manufacturing Sector
  - **Progress –** 3 collaborator installations completed with both network and agent based solutions considered
  - **Timeline**: draft NCCoE practice guide (SP 1800-10) due out in May, 2018
- **Next Up: Manufacturing Application Whitelisting**
  - Projected start: Summer 2018
  - Will include new collaborators

NCCOE ENERGY SECTOR UPCOMING ACTIVITIES

- **Winter 2018**
  - Industrial Internet Consortium Global Event Series, McLean, VA February 9. NCCoE energy team will have a booth. www.iiconsortium.org/reston-forum-2018

- **Spring 2018**
  - ICSJWG Spring 2018 Spring Meeting, Albuquerque, NM, April 10-12
    Call for abstracts pending, NCCoE plans to submit for speaking slot
  - NCCoE Spring 2018 Energy Sector Roundtable / Workshop
    General objective is to generate ideas for new projects, details are pending and EPC will be asked to provide input, attend, etc.

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

Contact Us

Jim McCarthy, Senior Security Engineer

Energy Sector Lead

James.McCarthy@nist.gov

301-975-0228

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov

About NCCoE

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.