

Energy Provider Community of Interest

November 24, 2015

Securing Networked Infrastructure for the Energy Sector

Agenda

- Current project overview
 - Identity and Access Management (IdAM) project update
 - NIST Washington Editorial Review Board (WERB)
 - Situational Awareness (SA) project update
- Project Pipeline

Identity and Access Management (IdAM) Use Case:

- Provides a reference solution to:
 - Authenticate individuals and systems
 - Enforce authorization control policies
 - Unify IdAM services
 - Protect generation, transmission and distribution
- Draft Practice Guide released August 25, 2015
- Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam
- Demonstrations available in NCCoE lab or on site
- Final Guide publication in February/ March 2016 timeframe
 - WERB membership request



*Centralized
management of silos*

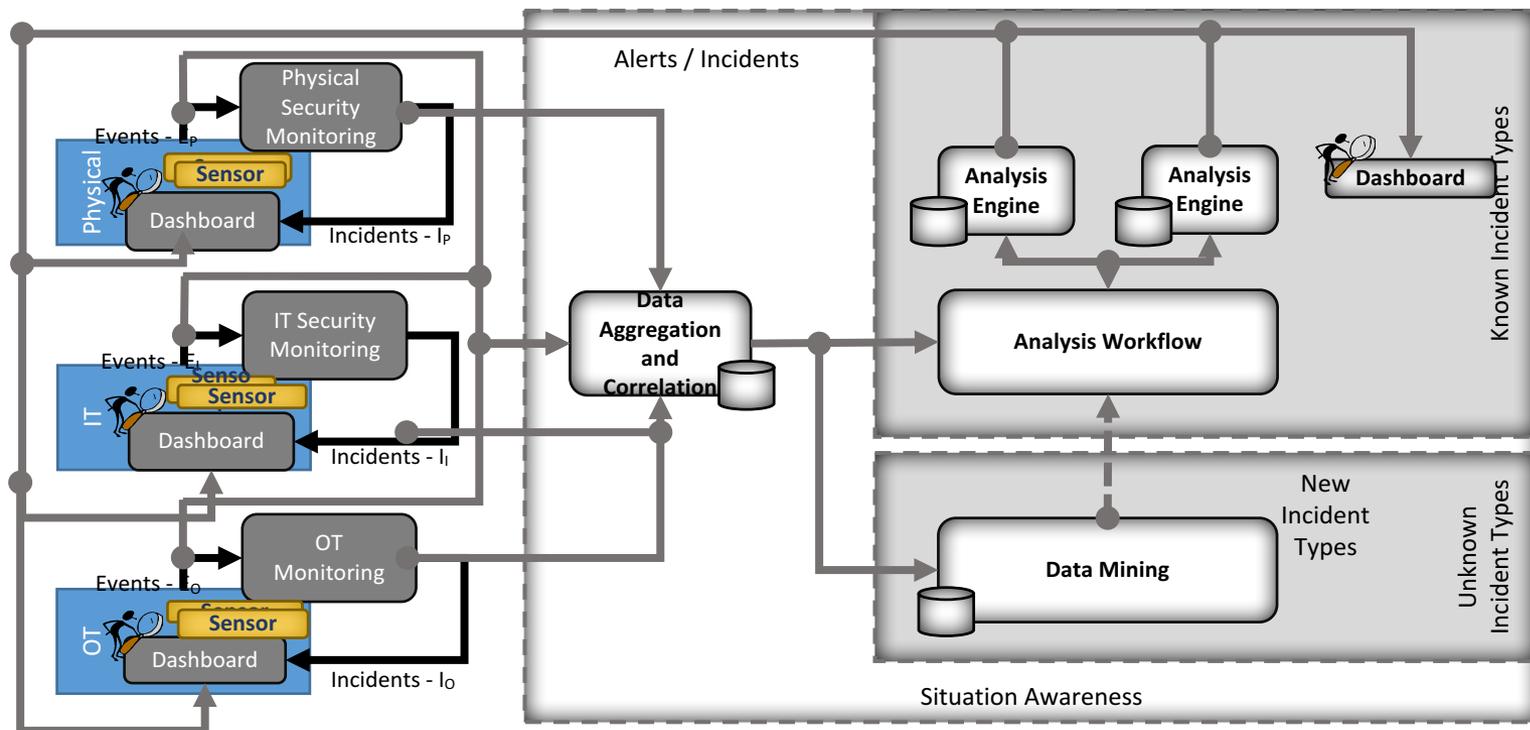


Adoption Activities

- ▶ Seeking pilot opportunities
- ▶ Increased engagement with industry integrators and trade associations
- ▶ Opportunities for COI members:
 - ▶ Demonstration of solution for your organization
 - ▶ Solution feasibility discussions
 - ▶ Industry vendor/ integrator introductions
 - ▶ COI outreach support

Situational Awareness

- ▶ Improve OT availability
- ▶ Detect anomalous conditions and remediation
- ▶ Investigate events leading to anomalies and share findings
- ▶ Unify visibility across silos



- 1) **OT – PACS event correlation**: sub-station/control station accessed and RTU, PLC goes down. Alert of anomalous condition and subsequent correlation to PACS to see who accessed facility.
Possible Option - if we set-up a virtual fence using a video system. We could correlate changes at the PLC to authorized and un-authorized accessed.

- 2) **IT – OT event correlation**: corporate billing app communicating with OT and could serve as a potential vector for attack. Unauthorized access from billing app (IT) to OT (malicious or inadvertent).

- 3) **IT – OT event correlation**: monitor the SCADA network for IP addresses that are outside of the pre-defined SCADA ranges. Monitor for connection requests from a device on the SCADA network destined for an IP that is outside of the SCADA IP ranges.
Option 1- Attempted external penetration from malicious actor
Option 2 – Implant of USB with Malware (Trojan ?) to open up communication path for external control of Operational Technology devices

- ▶ Use Case Published:
http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf
- ▶ Build Team Kickoff: 10/20/2015
- ▶ Components installed in Lab: 12/2015
- ▶ Systems Integration: 1/2016 – 3/2016
- ▶ Draft Practice Guide Release: 3/2016



*DRIVING TO RELEASE DATE
TO FACILITATE NERC CIP
COMPLIANCE*



- ▶ What keeps you up at night?
- ▶ On which problem(s) should we focus our efforts?

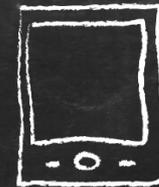
240-314-6800

<http://nccoe.nist.gov/forums/energy>



Thank You

energy_nccoe@nist.gov



9600 Gudelsky Drive
Rockville, MD 20850

ABOUT THE NCCOE

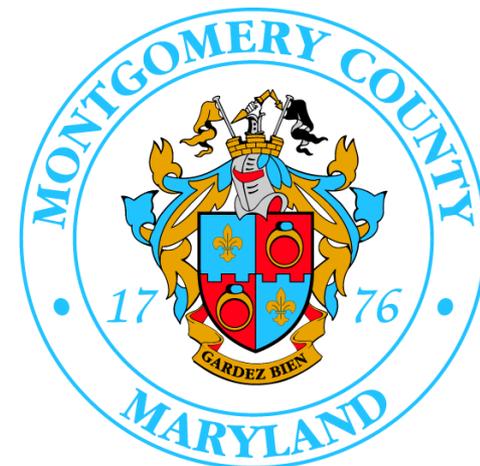


NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®

Department of Business & Economic Development





VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs



GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- ▶ Broadly applicable across much of a sector, or across sectors
- ▶ Addressable through one or more reference designs built in our labs
- ▶ Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- ▶ Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- ▶ Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)



Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards



Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications



Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions



Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry



Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

