

Energy Provider Community of Interest

March 8, 2016

Securing Networked Infrastructure for the Energy Sector

Agenda

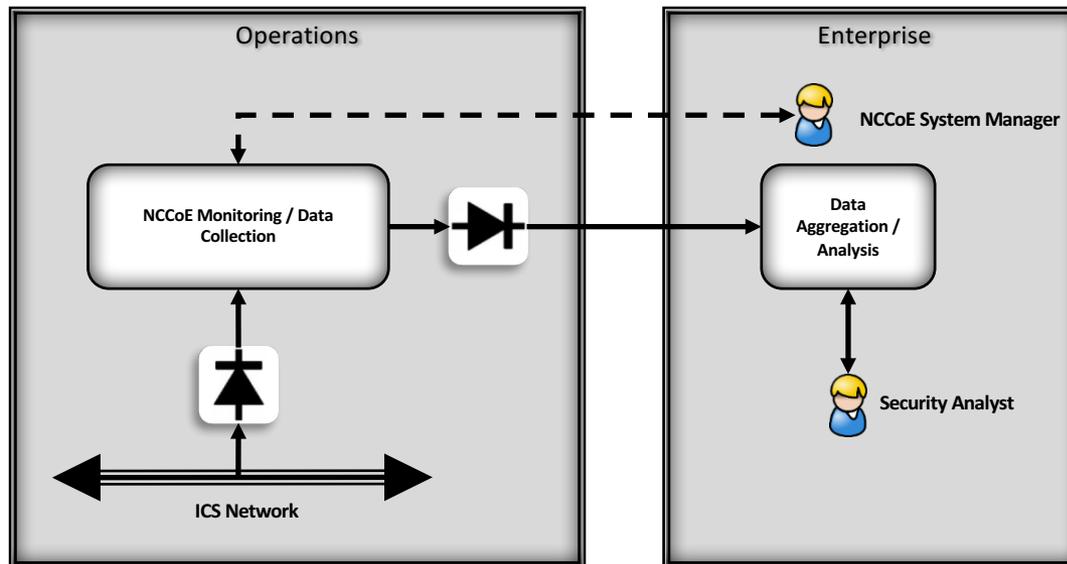
- NCCoE News
- Current Project Overview
 - Situational Awareness (SA) project update
 - Test cases
 - Identity and Access Management (IdAM) project update
- Open Discussion – NERC CIP v5 compliance date delay

NCCoE Out and About:

- Upcoming planned conferences
 - RSA (Feb) – *met with build team partners and security industry leaders*
 - UTC & Technology (May) – *Nate Lesser speaking*
 - ICS JWG (May) – *Jim McCarthy speaking*
 - APPA National Conference (June)
 - EnergySec (August)
 - Power Grid Cyber Security Exchange (August)
 - ICS Cybersecurity Conference Sacramento (October)
 - GridSecCon (October)
 - World Congress on Industrial Control Systems Security (WCICSS) (December)
- Upcoming planned visits
 - Black & Veatch

Situational Awareness Project

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



Situational Awareness Project Notional Test Case Scenarios

1	OT - PACS event correlation	<p>Sub-station/control station accessed. RTU at PLC goes down. Alert of anomalous condition and subsequent correlation to PACS to see who accessed facility.</p> <p>Possible Option - set-up a virtual fence using a video system in order to correlate changes at the PLC to authorized and un-authorized access</p>
2	IT - OT event correlation	<p>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).</p>
3	IT – OT event correlation	<p>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 range</p> <p>Option 1- Attempted external penetration from malicious actor</p> <p>Option 2 – Implant of USB with Malware (Trojan?) to open up communication path for external control of Operational Technology devices</p>
4	Report generation	<p>Demonstrate report generation to show regulatory compliance with CIP v5.</p>

Situational Awareness Project Milestones

- ▶ 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 in new lab: 1/2016 – 3/2016
- ▶ Completed build: 4/2016
- ▶ Draft Practice Guide release: 5/2016
- ▶ Early adoption: 5/2016 and ongoing
- ▶ Demonstrations: 5/2016 and ongoing
- ▶ Final Practice Guide release: 7/30/2016

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
 - Improve awareness and management of visitor accesses
 - Simplify the reporting process
- Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam
- Final Guide publication March 2016 timeframe
- Demonstrations and adoption support available



*Converged
management of silos*



IdAM Adoption Activities

- ▶ Continue to seek early adoption opportunities
- ▶ Increased engagement with industry utilities and integrators
- ▶ Opportunities for COI members:
 - ▶ Demonstration of solution for your organization
 - ▶ Solution feasibility discussions
 - ▶ Industry vendor/ integrator introductions
 - ▶ COI outreach support

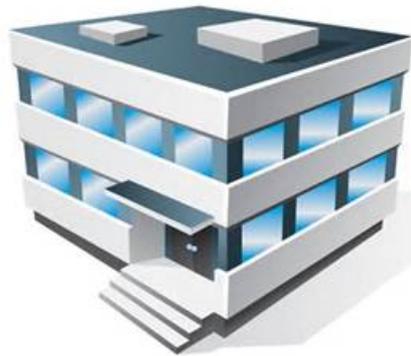
Contact us for more information!



- ▶ The NERC CIP v5 compliance date has been extended. What are the implications of this extension for your organization?



240-314-6800

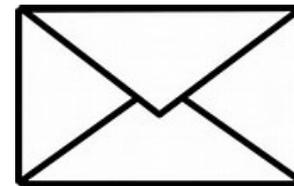


9700 Great Seneca Hwy,
Rockville, MD 20850

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



energy_nccoe@nist.gov



100 Bureau Drive, Mail Stop
2002, Gaithersburg, MD 20899

Thank You

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

