

# Energy Provider Community of Interest

## October 27, 2015

Securing Networked Infrastructure for the Energy Sector

## Monthly Call Agenda

- Current project overview
- Identity and Access Management (IdAM) project update
  - Update on adoption activities
- Situational Awareness (SA) project update
  - Updated architecture
  - Test case review for practicality
  - Request for dataset
- Conference attendance and outreach activities

## Identity and Access Management (IdAM)

- ▶ Authenticate individuals and systems
- ▶ Enforce authorization control policies
- ▶ Unify IdAM services
- ▶ Protect generation, transmission and distribution

## Identity and Access Management (IdAM) Draft Practice Guide Update

- ▶ Draft practice guide released August 25!
- ▶ Draft guide is online at [https://nccoe.nist.gov/projects/use\\_cases/idam](https://nccoe.nist.gov/projects/use_cases/idam)
- ▶ Statistics update
  - ▶ IdAM project web page visits since posted: 3,424
  - ▶ IdAM Guide Downloads
    - ▶ Total downloads since release: 3,565
    - ▶ Total downloads by section/file
      - ▶ 1800-2a Executive Summary: 750
      - ▶ 1800-2b Approach: 716
      - ▶ 1800-2c How-To Guide: 581
      - ▶ ES IdAM Use Case (zip file): 759

## Adoption Activities

- ▶ First Pilot opportunity identified and coordination underway
- ▶ Increased engagement with industry integrators
- ▶ Opportunities for COI members:
  - ▶ Demonstration of solution for your organization
  - ▶ Solution feasibility discussions
  - ▶ Industry vendor/ integrator introductions
  - ▶ COI outreach support
    - ▶ Email copy available for you to send to your colleagues
    - ▶ Social media posts available for you to use

## Usability Study of NIST SP1800-2

Conducted by Drs. Sarah Kriz & Deanna Caputo

The MITRE Corporation

**Seeking interview candidates familiar with the NCCoE IdAM practice guide:**

- ▶ CIOs, CISOs, managers, and integrators from electric utilities
- ▶ Industry integrators
- ▶ IdAM vendors

**Areas of focus for feedback:**

- ▶ Usability of the practice guide document
- ▶ Feasibility of the IdAM solution

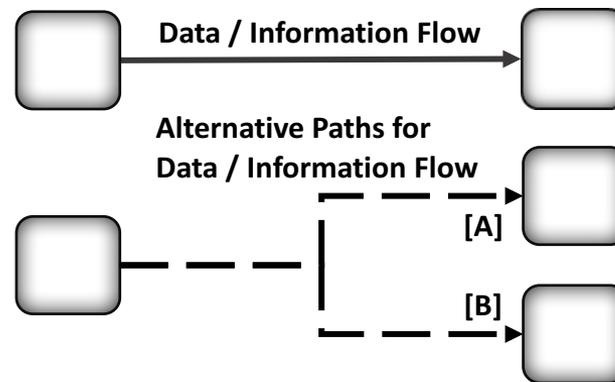
**Contact Dr. Sarah Kriz**

[skriz@mitre.org](mailto:skriz@mitre.org)

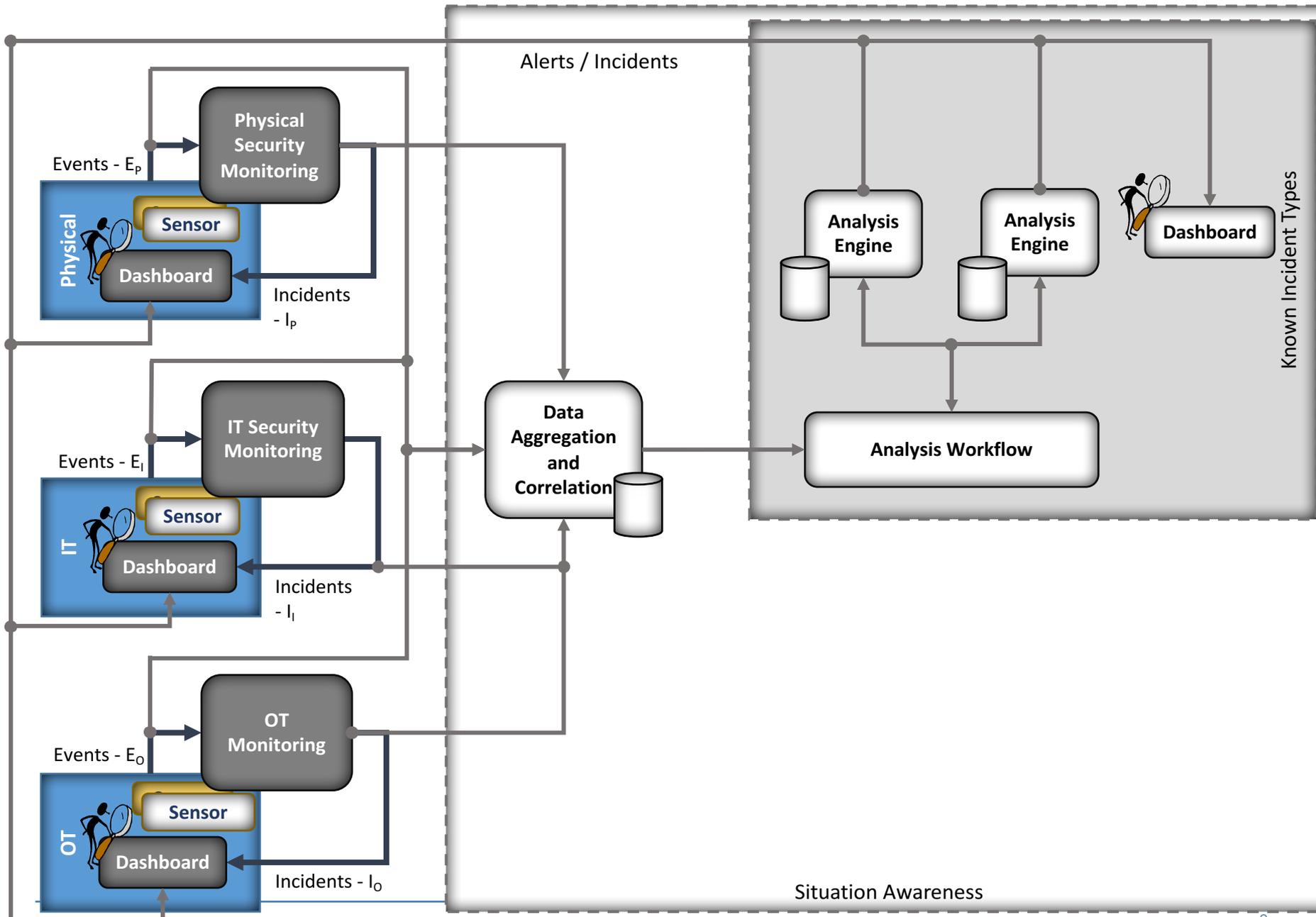
**703-983-0470**

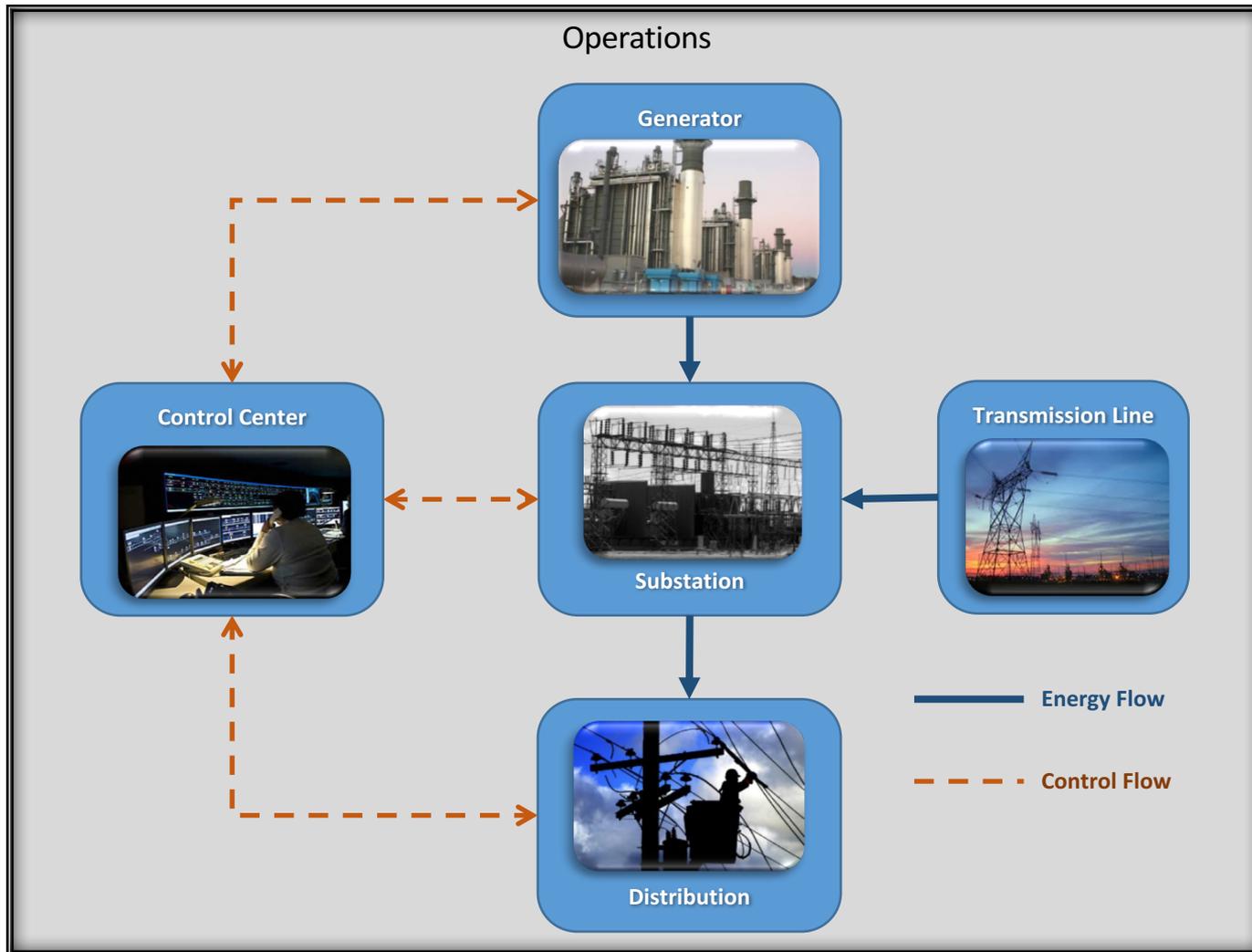
## Situational Awareness

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

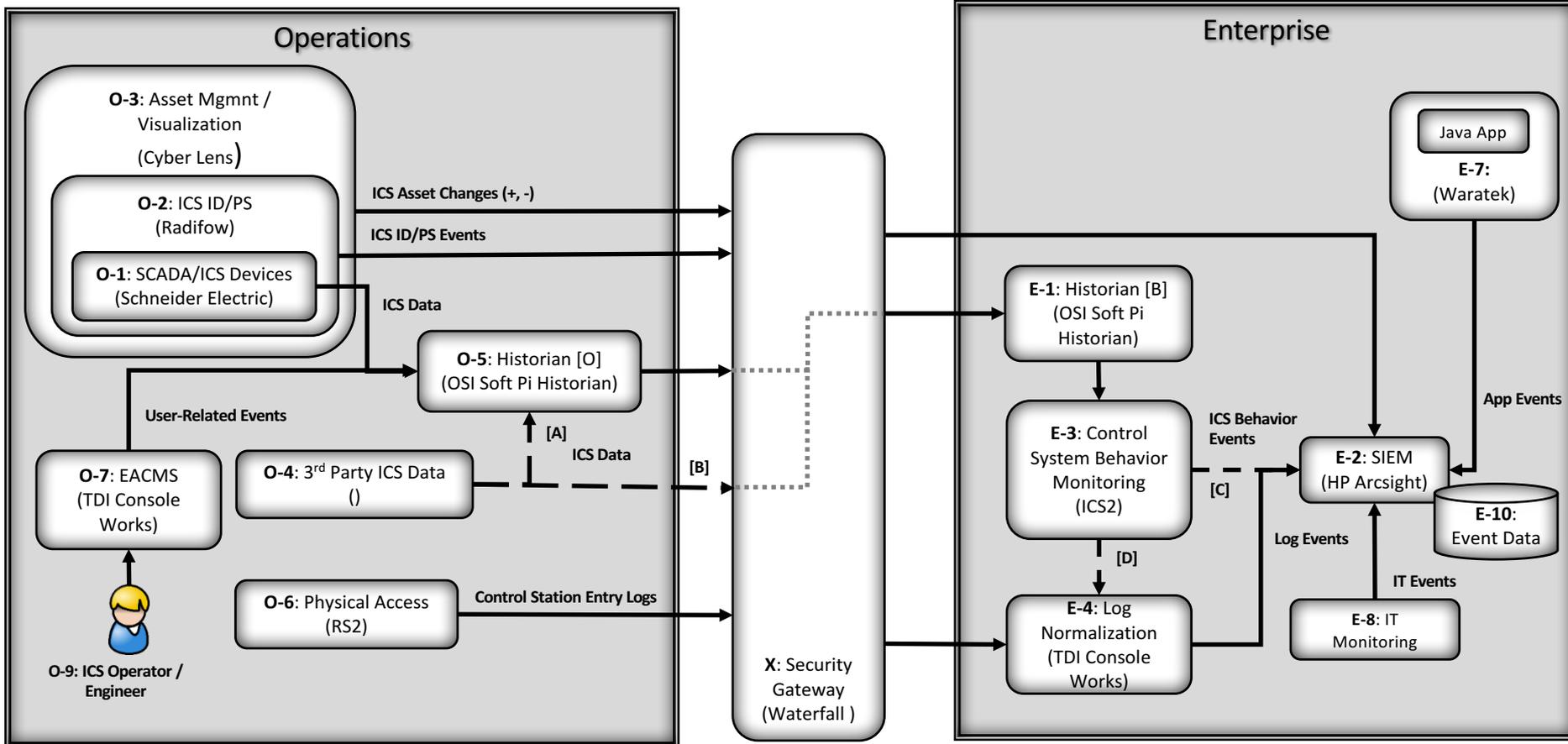


# SITUATIONAL AWARENESS: CENTRALIZED MANAGEMENT



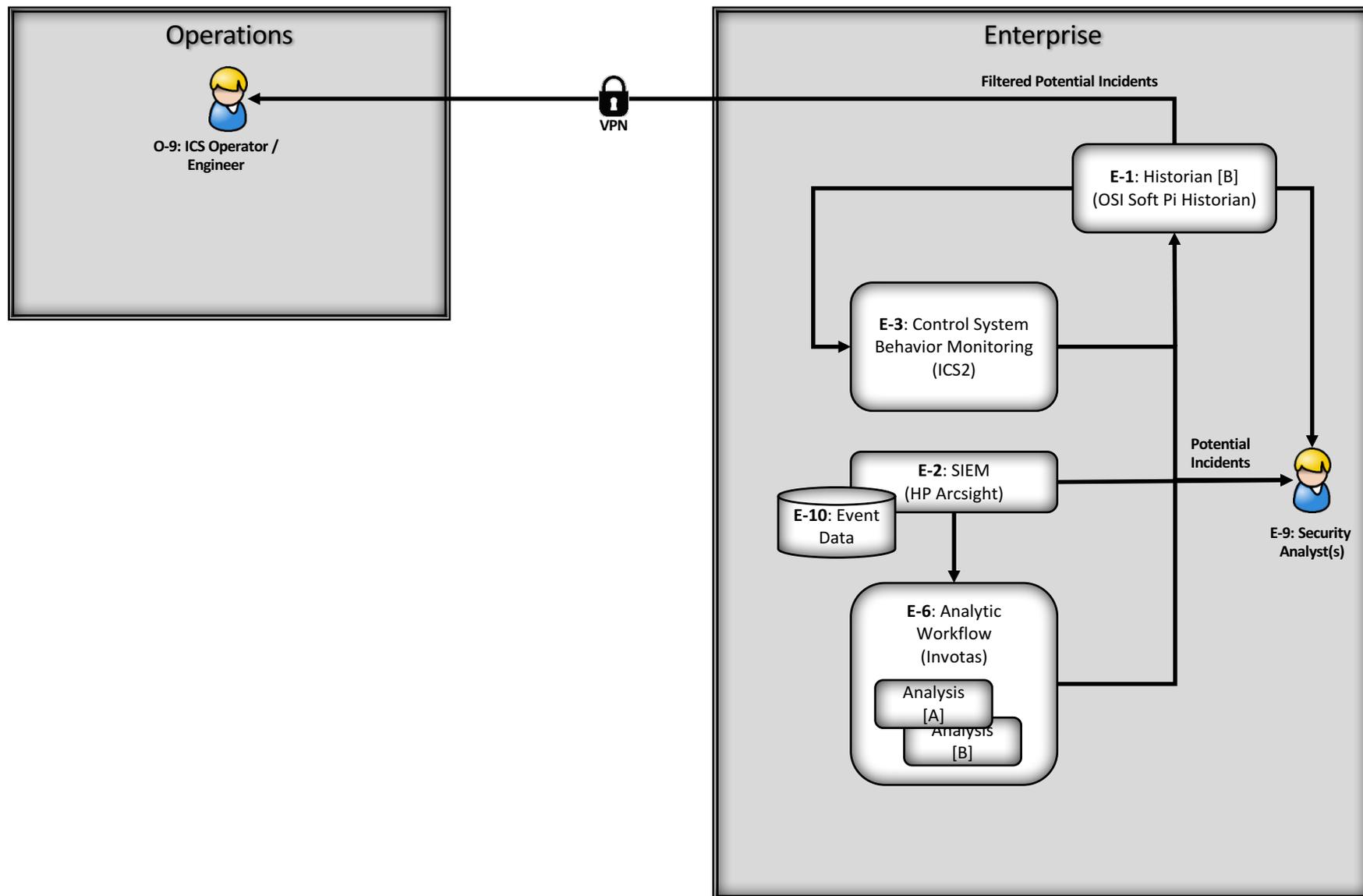


Company Name	Capability / Type	Enterprise	Operations	Purpose
Waterfall Security	Security gateway	X	X	One way transfer device
Waratek	Real time app vulnerability detection	X		Application layer security in IT enclave. Endpoint based detection.
ICS2	ICS Data Analytics, ICS anomaly detection	X		Monitoring of process control data flows
Inventas	ICS data analytics and automated workflow remediation	Analytic Enclave		Automation of analytic workflow/ remediation
Radiflow	ICS IDS		X	Intrusion detection for the OT network
Dragos Security / Cyber Lens	ICS Asset Management, ICS Data Analytics, ICS anomaly detection		X	Asset identification management/identification and anomaly detection
OSIsoft	Pi Historian	X	X	Data historian
HP/ ArcSight	SIEM, Aggregation, correlation	Analytic Enclave		SIEM
Schneider Electric	ICS Gear		X	ICS Firewall
TDI Technologies / Console Works	Logging for IT/OT devices	Analytic Enclave		Log aggregation platform and data log integrity checking / vendor management
RS2 Technologies	PACS		X	Door controller



- O-1 Supervisory Control And Data Acquisition / Industrial Control System (SCADA/ICS) devices are responsible for monitoring and controlling electricity generation and distribution.
- O-2 ICS Intrusion Detection and Prevention System (ID/PS) monitors ICS traffic, identifies anomalous traffic and prevents traffic known to be inappropriate
- O-3 ICS Asset Management monitors ICS traffic to detect the addition/removal of ICS devices
- O-4 Third Party ICS data is ICS monitoring data provided by contractor operating generation and distribution
- O-5 is the operations historian that collects and stores ICS data
- O-6 is the physical access control system for generation, transmission substation, and the control center
- O-7 is the Electronic Access Control and Monitoring System (EACMS) that controls O-9, interactive user access to ICS devices
- X is a Security Gateway that provides one-way data flow from Operations to Enterprise
- E-1 is the enterprise historian that stores replicas of ICS data collected in Operations
- E-2 is a Security Information Event Management (SIEM) system that collects, normalizes, and correlates security-related event information from sources across Operations, IT, and physical security
- E-3 is a sensor that detects anomalous control system behavior by examining ICS data from a historian
- E-4 is a log aggregator
- E-7 is an application monitoring system that reports unusual application behavior as a security-related event
- E-8 provides security-related event information from IT monitoring

- O-1 SCADA/ICS devices send data to O-5, the Operations historian for storage
- O-4 Third Party ICS Data is sent to either
  - O-5, the operations historian
  - E-1, the enterprise historian, via X, the security gateway
- O-2 sends reports of anomalous ICS network traffic to E-2, the SIEM, via X the security gateway
  - If necessary, this data may, instead, be sent to E-4, log normalization, for preprocessing prior to being sent to E-2
- O-3 sends reports ICS devices added to or removed from the ICS network to E-2, the SIEM, via X, the security gateway
  - If necessary, this data may, instead, be sent to E-4, log normalization, for preprocessing prior to being sent to E-2
- O-5, the operations historian, replicates the data it receives to E-1, the enterprise historian via X, the security gateway
- O-6, physical access control sends log data to E-4, log normalization, which processes the records and sends them to E-2, the SIEM
- O-7, the EACMS, sends reports of inappropriate interactive user activity to O-5, the operations historian
- E-3, the control system behavioral monitoring system reads data from E-1, the enterprise historian, and analyses it to identify any process-level anomalies control system behavior
  - E-3 sends any detected anomalies to E-2, the SIEM
- E-7, application monitoring, reports any application behavior anomalies to E-2, the SIEM
- E-8, IT monitoring, reports any IT system or network anomalies to E-2, the SIEM



- E-2, the SIEM aggregates event data from multiple sources and performs correlations to identify potential incidents.
  - E-9, security analysts are notified of potential incidents
- E-6 analytic workflow receives event and potential incident data from E-2 the SIEM. E-6 uses this data to automatically trigger analysis actions
  - Analysis provides potential incident information to E-9 security analysts
- E-3, the control system behavioral monitoring system reads data from E-1, the enterprise historian, and analyses it to identify any process-level anomalies control system behavior
  - E-3 provides potential incident information to E-9, security analysts
- E-3, the control system behavioral monitoring system, E-2, the SIEM, and E-6, analytic workflow, provide potential incident information to E-1, the enterprise historian, which filters the potential incident information and provides relevant information to O-9 operators and engineers

- Synthesized events will be injected into collection and analysis to demonstrate situational awareness across OT, PACS, and IT

- 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

- NCCoE would like to capture SCADA network and historian data sets from real utility environments for use in our SA lab build.
- The purpose is to analyze the data set for anomalies that may or may not have been detected by the data set owner.
- Additionally we will be attempting to design situational awareness visualizations/reporting that reduces the time needed for a security analysts to respond to similar events.
- Data may be anonymized for privacy concerns – the owner may decide if the findings should be publicized in the practice guide.

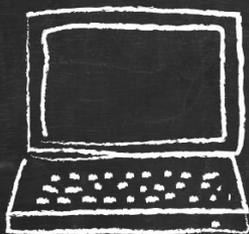
<b>DistribuTECH</b>	<b>Orlando, FL</b>
<b>GridSecCon</b>	<b>Philadelphia, PA</b>
<b>ICS Cybersecurity Conference</b>	<b>Atlanta, GA; London, UK</b>
<b>ICS Joint Working Group</b>	<b>Savannah, GA</b>
<b>Cyber Security Implementation Workshop</b>	<b>New Orleans, LA</b>
<b>Cybersecurity for ICS Canada</b>	<b>Calgary, Canada</b>
<b>World Congress on Industrial Control Systems Security (WCICSS)</b>	<b>London, UK</b>

240-314-6800

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



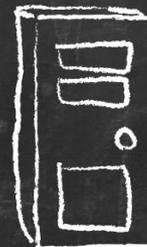
**Thank You**



[energy\\_nccoe@nist.gov](mailto:energy_nccoe@nist.gov)



9600 Gudelsky Drive  
Rockville, MD 20850



# ABOUT THE NCCOE

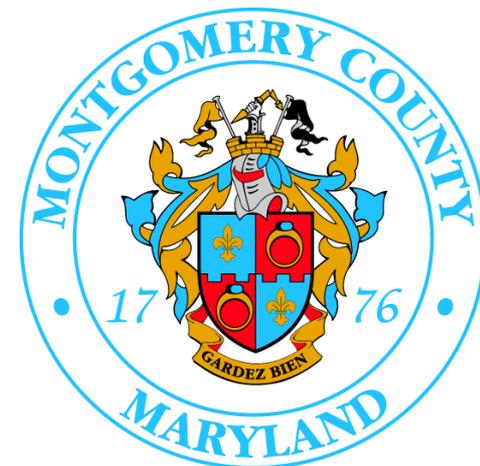


**NIST**  
**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

## 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

