National Cybersecurity Center of Excellence (NCCoE)
Energy Sector

Energy Provider Community of Interest

20 December 2016

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE Energy Sector News
  - New NCCoE Planned Activities

- Energy Sector Project Updates
  - Identity and Access Management (IdAM) Project Update
  - Situational Awareness (SA) Project Update
  - NCCoE Cybersecurity for Manufacturing
  - Supply Chain Use Case Development
  - Overall Year End Status
- EPC Open Discussion / Comments / Questions

YEAR END STATUS – ENERGY SECTOR PROJECTS

- Identity and Access Management SP 1800-2 (a,b,c)
  - Draft released 08/25/2015
  - All comments adjudicated by 05/2016
  - Delay – use of logos in practice guide, nearing resolution
  - Washington Executive Review Board (WERB)
  - Projected release of final; 01/2017

- Situational Awareness SP 1800-7 (a,b,c)
  - Build complete (NCCoE and UMd)
  - Draft document submitted to build team for review
  - Projected public draft release; 01/2017

YEAR END STATUS – ENERGY SECTOR PROJECTS

- Cybersecurity for Manufacturing
  - Released draft project description 11/07/2016
  - Extended comment period to 12/22/2016
  - Comment adjudication – approx. 15 - 20 days
  - Final project description – late Jan. to early Feb., 2017

- Supply Chain (SC) Use Case Development
  - Initiated 09/2016, for Energy Sector
  - Challenge – use case needs to be based on Security capabilities / technologies, comport to NERC-CIP
  - Research – attended local Supply Chain workshops, workgroup meetings (week of 12/12/2016)
  - Established EPC SC Sub-Working Group (first meeting 12/16/2016)

EPC OPEN DISCUSSION

- Your thoughts

CONTACT US

301-975-0200

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

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850

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

Thank You

ABOUT THE NCCOE

FOUNDERS

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

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®

Department of Business & Economic Development

MONTGOMERY COUNTY
17 76
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

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)

TENETS

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

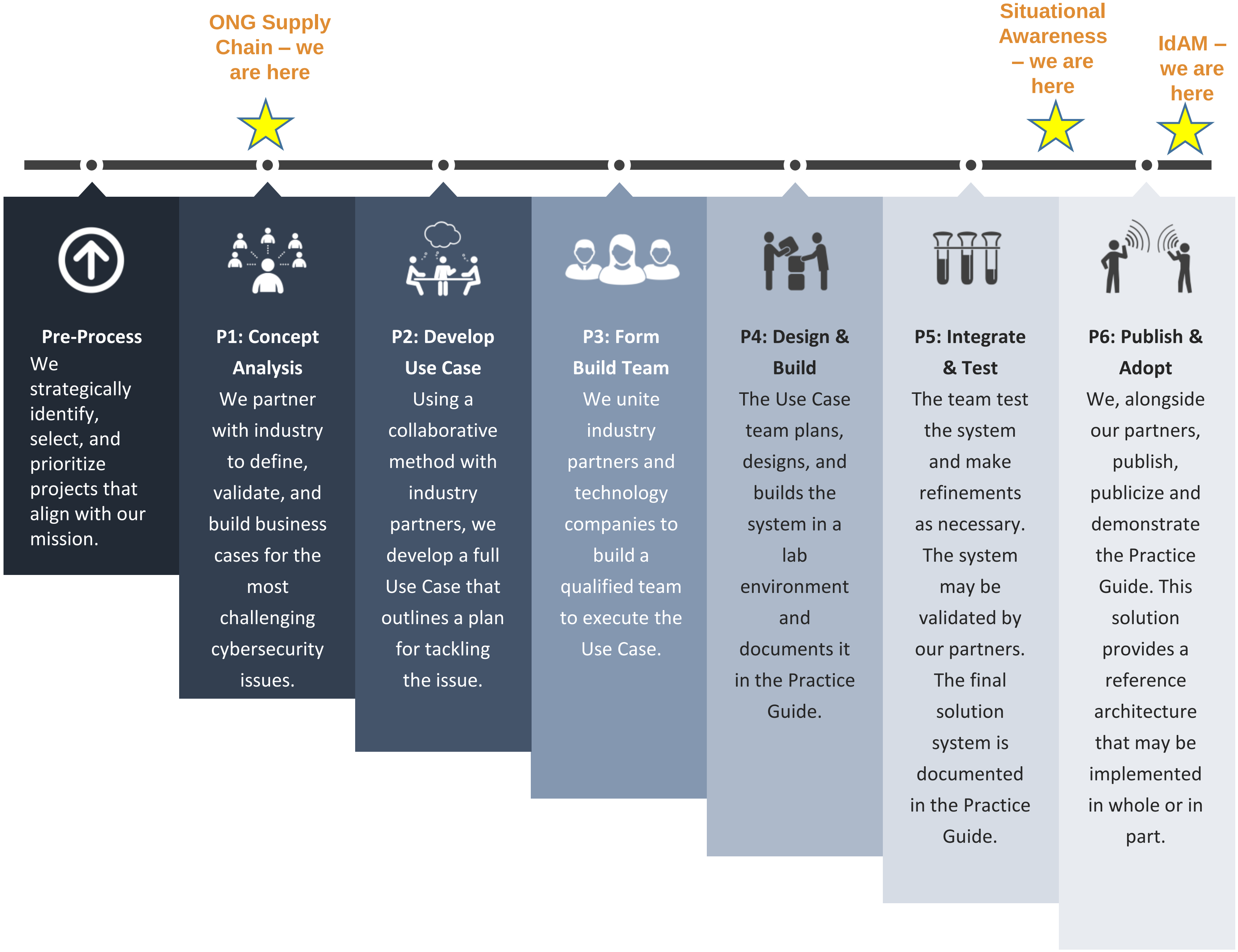
Usable

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

PROJECT PHASES



ONG Supply Chain – we are here

Situational Awareness – we are here

IdAM – we are here

Pre-Process
We strategically identify, select, and prioritize projects that align with our mission.

P1: Concept Analysis
We partner with industry to define, validate, and build business cases for the most challenging cybersecurity issues.

P2: Develop Use Case
Using a collaborative method with industry partners, we develop a full Use Case that outlines a plan for tackling the issue.

P3: Form Build Team
We unite industry partners and technology companies to build a qualified team to execute the Use Case.

P4: Design & Build
The Use Case team plans, designs, and builds the system in a lab environment and documents it in the Practice Guide.

P5: Integrate & Test
The team test the system and make refinements as necessary. The system may be validated by our partners. The final solution system is documented in the Practice Guide.

P6: Publish & Adopt
We, alongside our partners, publish, publicize and demonstrate the Practice Guide. This solution provides a reference architecture that may be implemented in whole or in part.

Icon Credits (right to left): Talking by Juan Pablo Bravo; Test Tube by Olivier Guin; Collaboration by Krisada; Team by Wilson Joseph; Brainstorm by Jessica Lock; Network by Matthew Hawdon; Arrow by Jamison Wieser; all from the Noun Project.

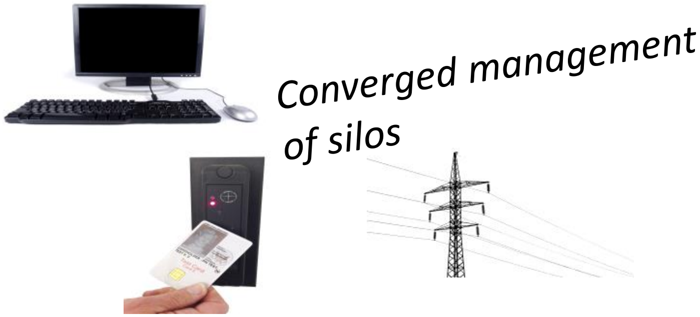
CURRENT PROJECTS: IDAM

Challenges we heard from industry:

- Lack of authentication, authorization, and access control requirements for all OT
- Inability to manage and log authentication, authorization, and access control information for all OT using centralized or federated controls
- Inability to centrally monitor authorized and unauthorized use of all OT and user accounts
- Inability to provision, modify, or revoke access throughout the enterprise (including OT) in a timely manner

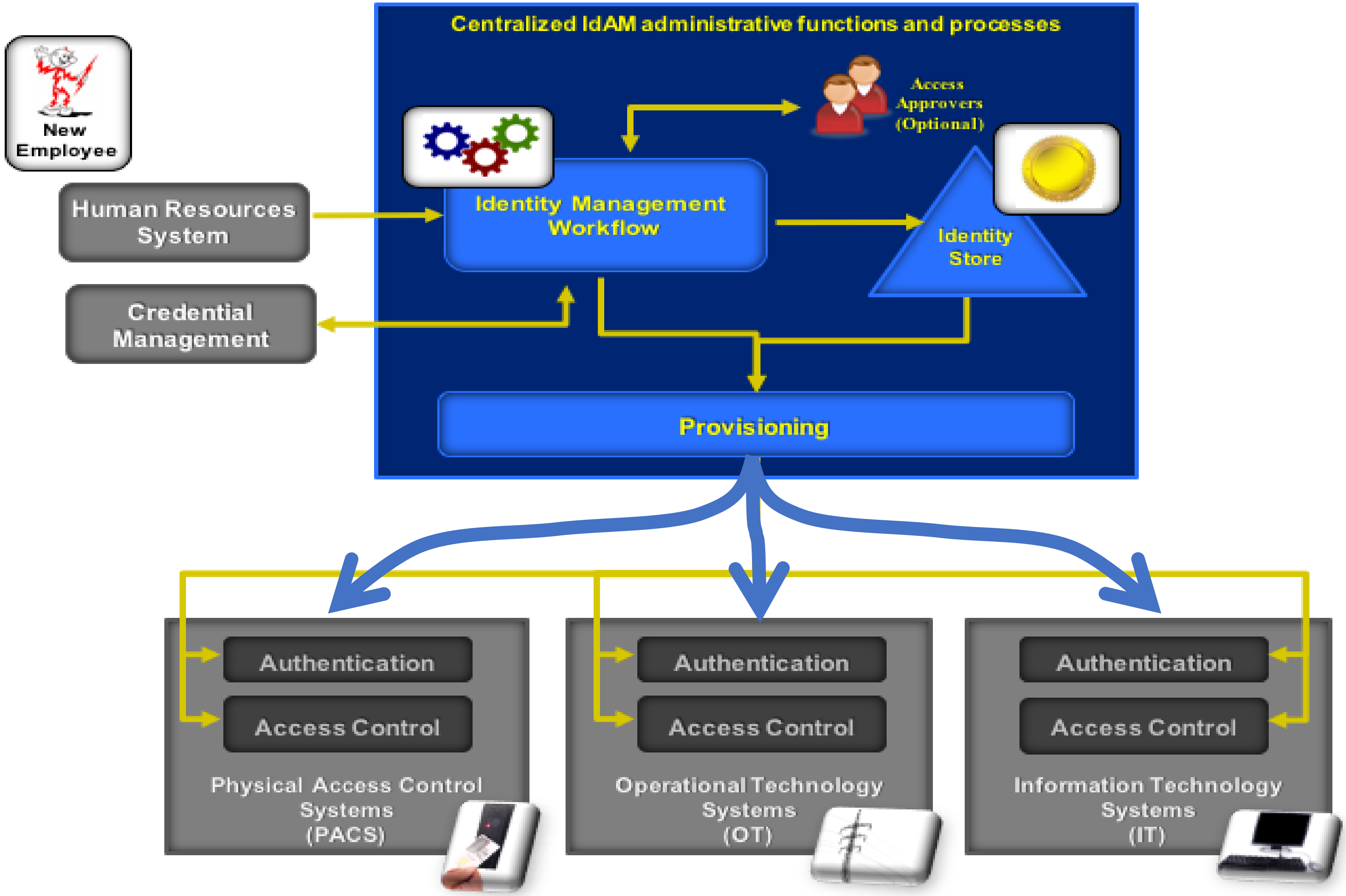
Solution NCCoE built:

- ✓ Authenticates individuals and systems
- ✓ Enforces authorization control policies
- ✓ Unifies IdAM services
- ✓ Protects generation, transmission and distribution
- ✓ Improves awareness and management of visitor accesses
- ✓ Simplifies the reporting process



Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam

CURRENT PROJECTS: IDAM SOLUTION


New Employee
Human Resources System
Credential Management
Centralized IdAM administrative functions and processes
Access Approvers (Optional)
Identity Management Workflow
Identity Store
Provisioning
Authentication
Access Control
Physical Access Control Systems (PACS)
Authentication
Access Control
Operational Technology Systems (OT)
Authentication
Access Control
Information Technology Systems (IT)

CPS Energy (San Antonio) and NCCoE are collaborating on a case study to document a worked example, lessons learned, and known benefits. Expect to complete by October.

CURRENT PROJECTS: SITUATIONAL AWARENESS

Industry Challenges:

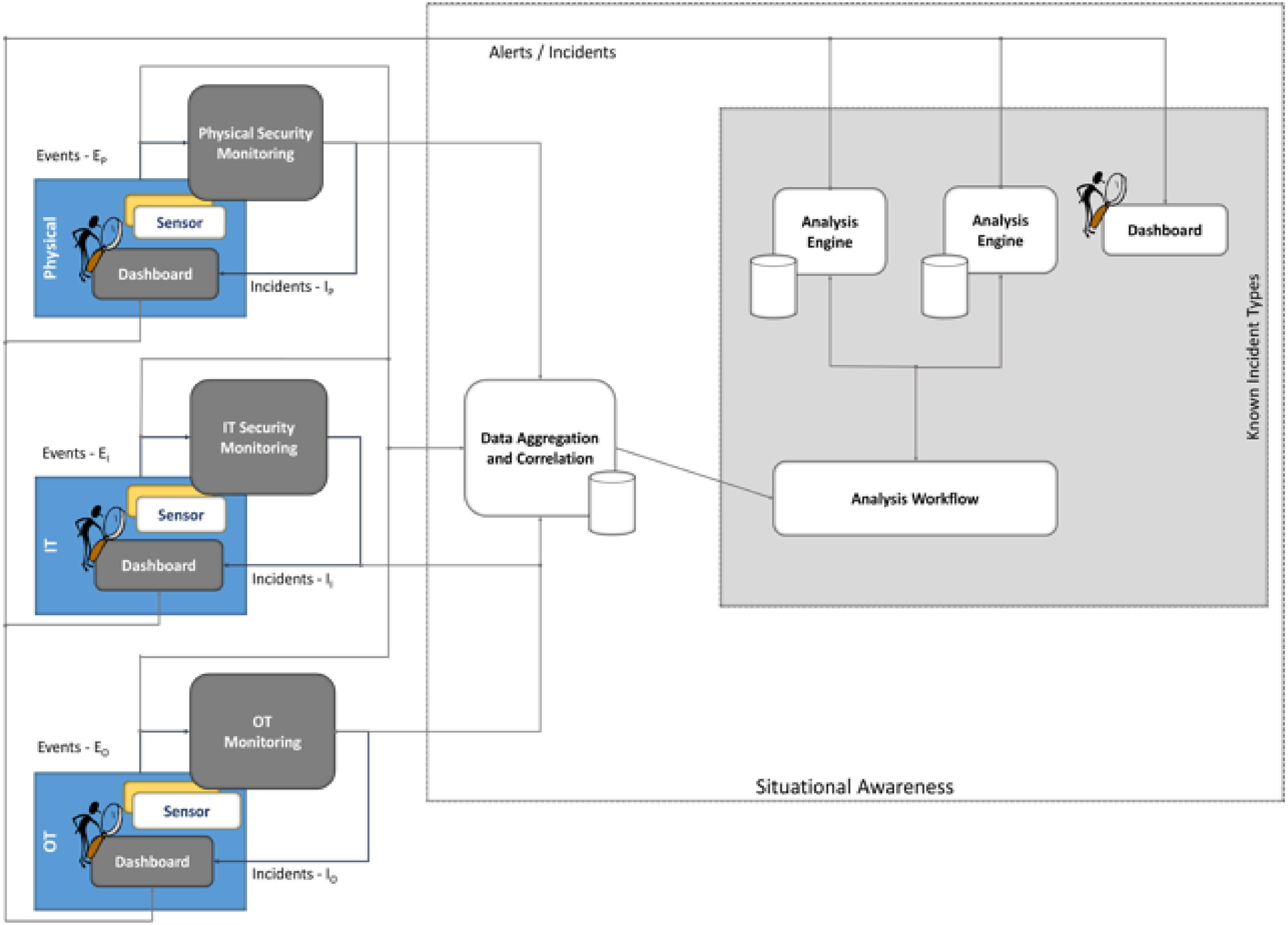
- Improve OT availability
- Detect anomalous conditions and remediation
- Unify visibility across silos
- Investigate events leading to baseline deviations/ anomalies
- Share findings

Solution NCCoE is developing:

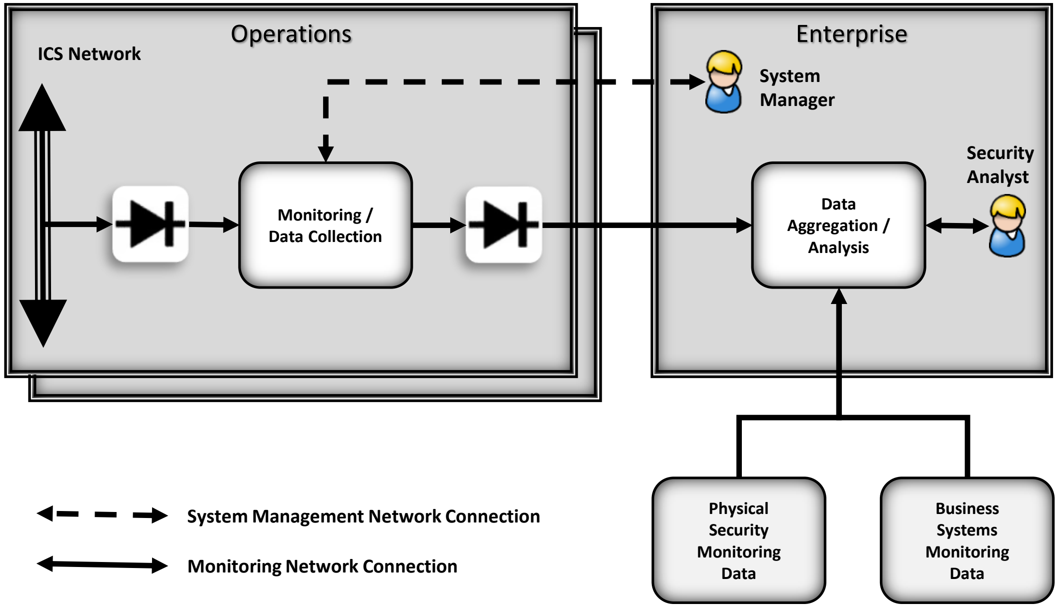
- ✓ Improves the ability to detect cyber-related security breaches or anomalous behavior
- ✓ Improves accountability and traceability
- ✓ Simplifies regulatory compliance by automating generation and collection of operational log data
- ✓ Increases the probability that investigations of attacks or anomalous system behavior will reach successful outcomes

Use Case is online at https://nccoe.nist.gov/projects/use_cases/situational_awareness

CURRENT PROJECTS: SITUATIONAL AWARENESS SOLUTION



CURRENT PROJECTS: SITUATIONAL AWARENESS



Operations
ICS Network
Monitoring / Data Collection
Enterprise
System Manager
Security Analyst
Data Aggregation / Analysis
Physical Security Monitoring Data
Business Systems Monitoring Data
System Management Network Connection
Monitoring Network Connection

- Collect data from an Operations facility that includes Industrial Control Systems (ICS)
  - Ensure data can only flow OUT of the ICS Network into the monitoring and collection hardware / software
- Send data collected from Operations to an Enterprise data aggregation and analysis capability
  - Operations data is aggregated with business systems monitoring data and physical security monitoring data
  - Ensure data can only flow OUT of Operations into Enterprise
- Use the aggregated data to provide converged situational awareness across Operations and Business systems as well as physical security of buildings and other facilities
- Provide a limited-access remote management path from Enterprise to Operations to manage monitoring / data collection hardware and software