Monthly Call Agenda

- IdAM project update and call to action
- Situation Awareness project update
  - Notional reference architecture
  - High level project lifecycle

Identity and Access Management (IdAM) Practice Guide Release

- Practice guide release today!
- Find the guide online at https://nccoe.nist.gov/projects/use_cases/idam
- Submit comments (deadline October 23):
  - Do you believe NCCoE has properly identified a serious security concern within the energy industry?
  - Does the practice guide effectively address a serious security concern *within your organization*?
  - What would be the biggest obstacle to adoption of this solution, as a whole or in part?
  - If the NCCoE were to consider subsequent iterations of this practice guide, what would you suggest as the core focus?

What's Next?

- Demonstration of solution
- Customized review of practice guide with your organization
- Are we doing good work? Help us get the word out!
  - Email copy available for you to send to your colleagues
  - Social media posts available for you to use

Contact us at energy_nccoe@nist.gov

Energy Sector Situation Awareness Use Case

Notional Reference Architecture

July 2015

What is Situation Awareness

- Situation awareness is “"the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future“
  - Endsley, M.R. (1995b). Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32–64
- “Cyber situational awareness involves the normalization, deconfliction, and correlation of disparate sensor data, and the ability to analyze data and display the results of these analyses.”
  - http://itlaw.wikia.com/wiki/Cyber_situational_awareness
- “More simply, it's knowing what is going on around you.”
  - https://www.uscg.mil/auxiliary/training/tct/chap5.pdf

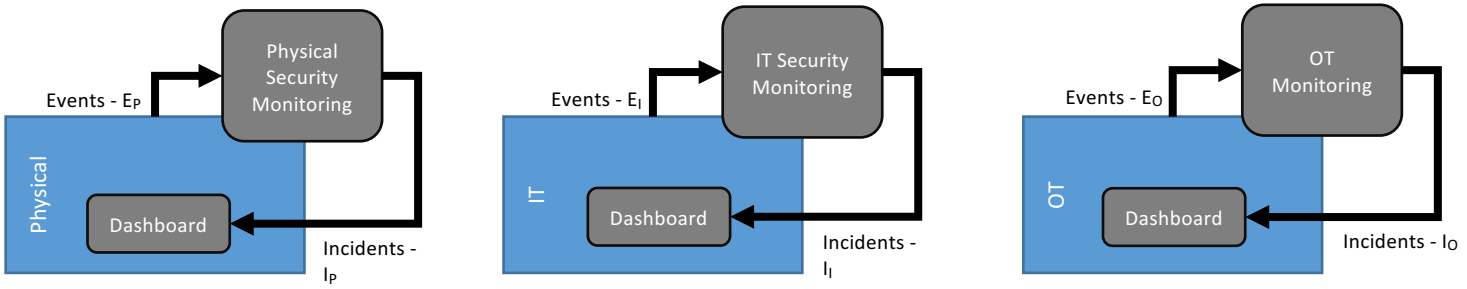
Energy Sector Situation Awareness Use Case

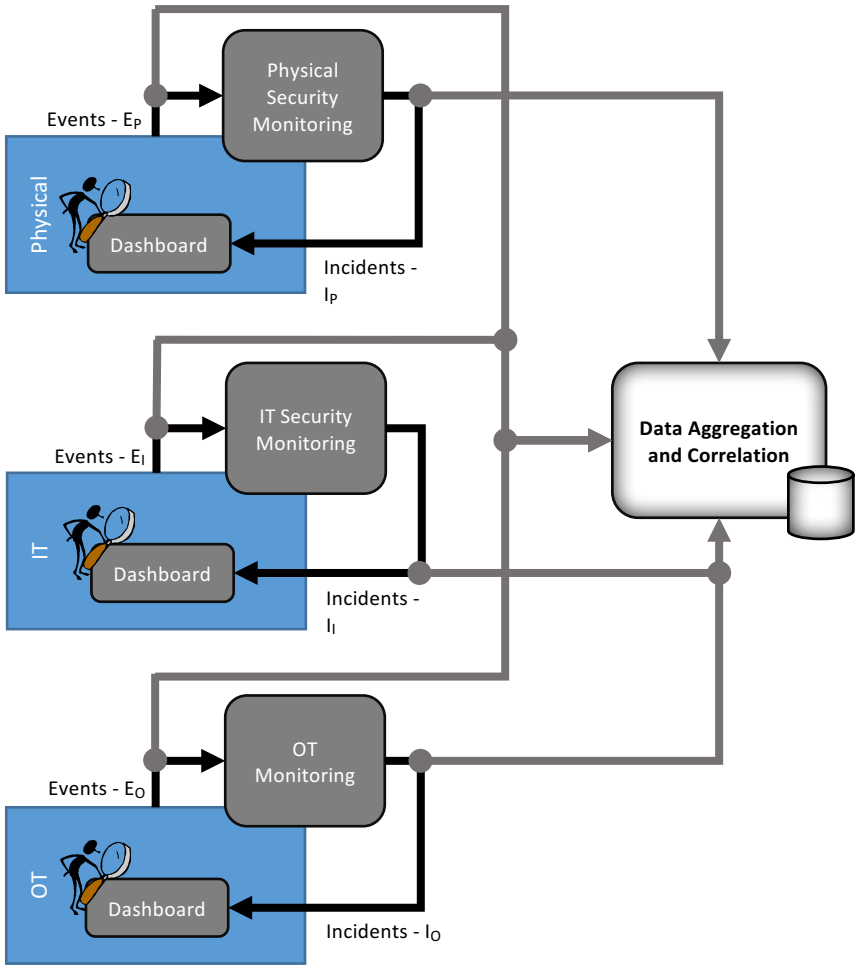
- Goal
  - Improve security of operational technology, using mechanisms that capture, transmit, analyze and store real-time or near-real-time data from industrial control systems (ICS) and related networking equipment.
- Some Desired Solution Characteristics
  - Analysis and correlation capabilities to help identify and understand security events and predict how they might affect control system operation
  - Analysis and visualization capabilities to help view control system behavior, network security events, and physical security events as a cohesive whole
  - Mechanisms that ensure the accuracy and integrity of data collected from remote faculties
  - Ability to automate common, repetitive investigative tasks

http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf

Assumptions

- Each silo, physical, IT, and OT have existing monitoring capabilities
  - These capabilities collect, correlate, and analyze events within a silo
  - Each silo detects and responds to incidents within the silo
  - Event and incident information is not shared among silos
- Incident detection can be improved by correlating and analyzing event and incident data across silos





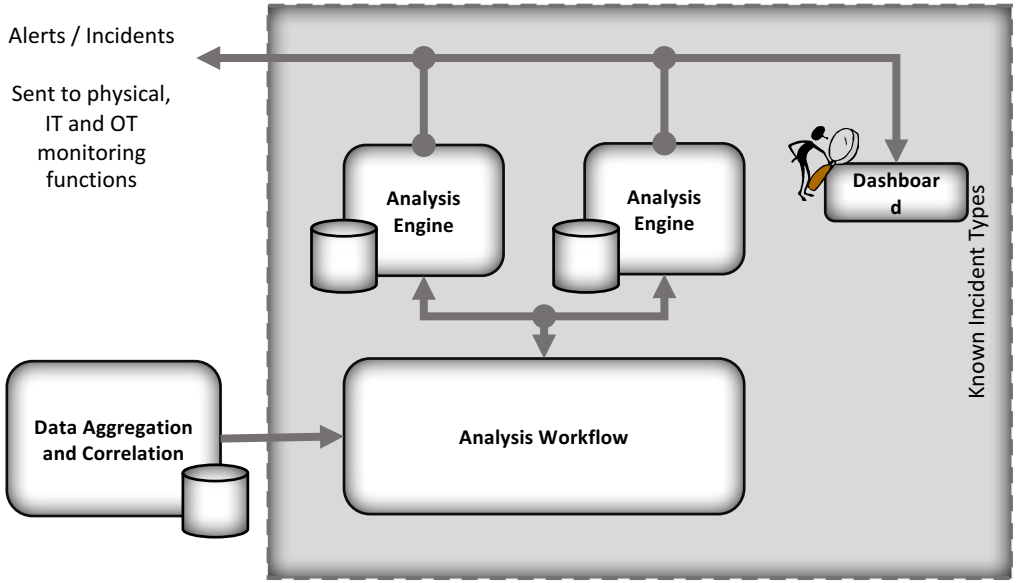
Step One

Aggregate, normalize, and correlate existing data from all three silos

Step Two

Apply analytic tools to the aggregated data to detect know incident types

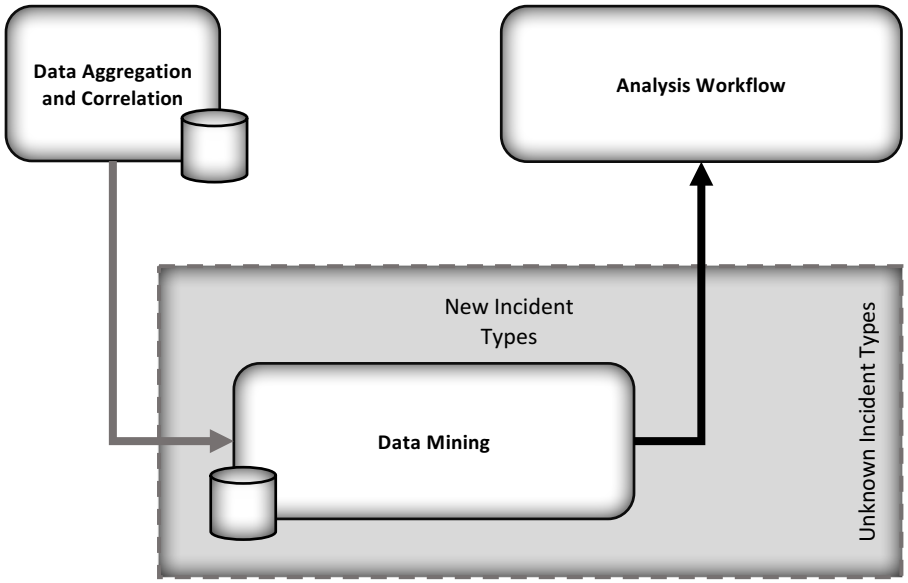
Automate the application of analytic tools where possible

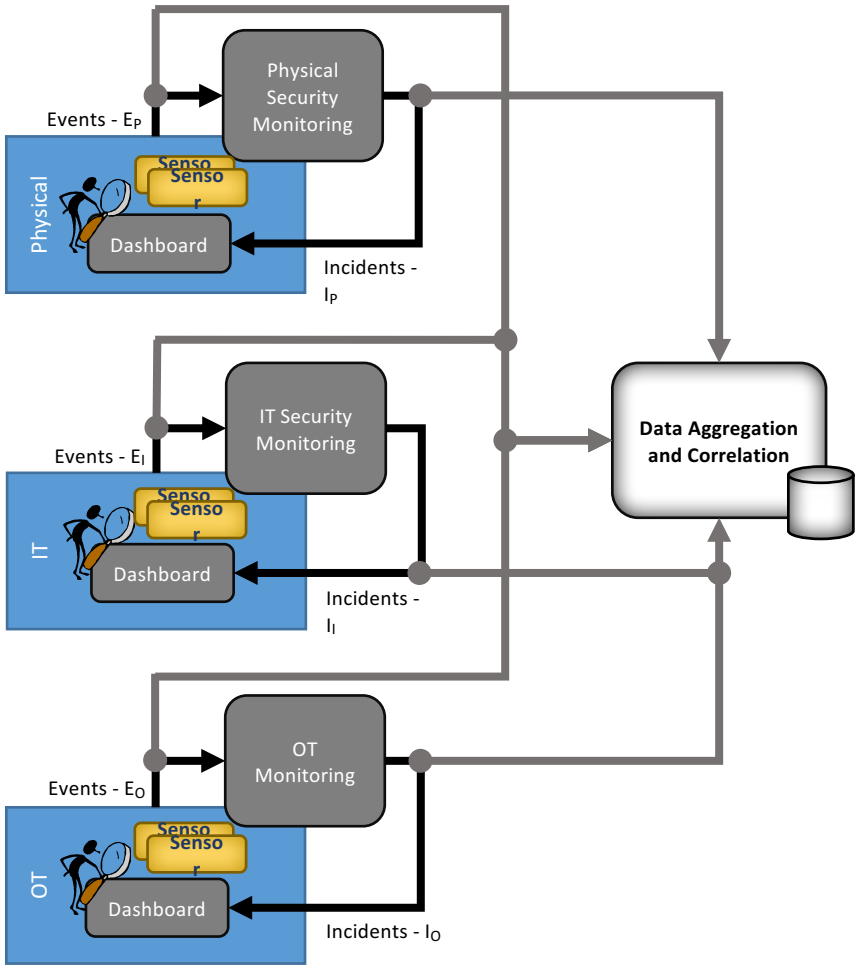


Step Three

Mine aggregated data to find previously unknown incident types

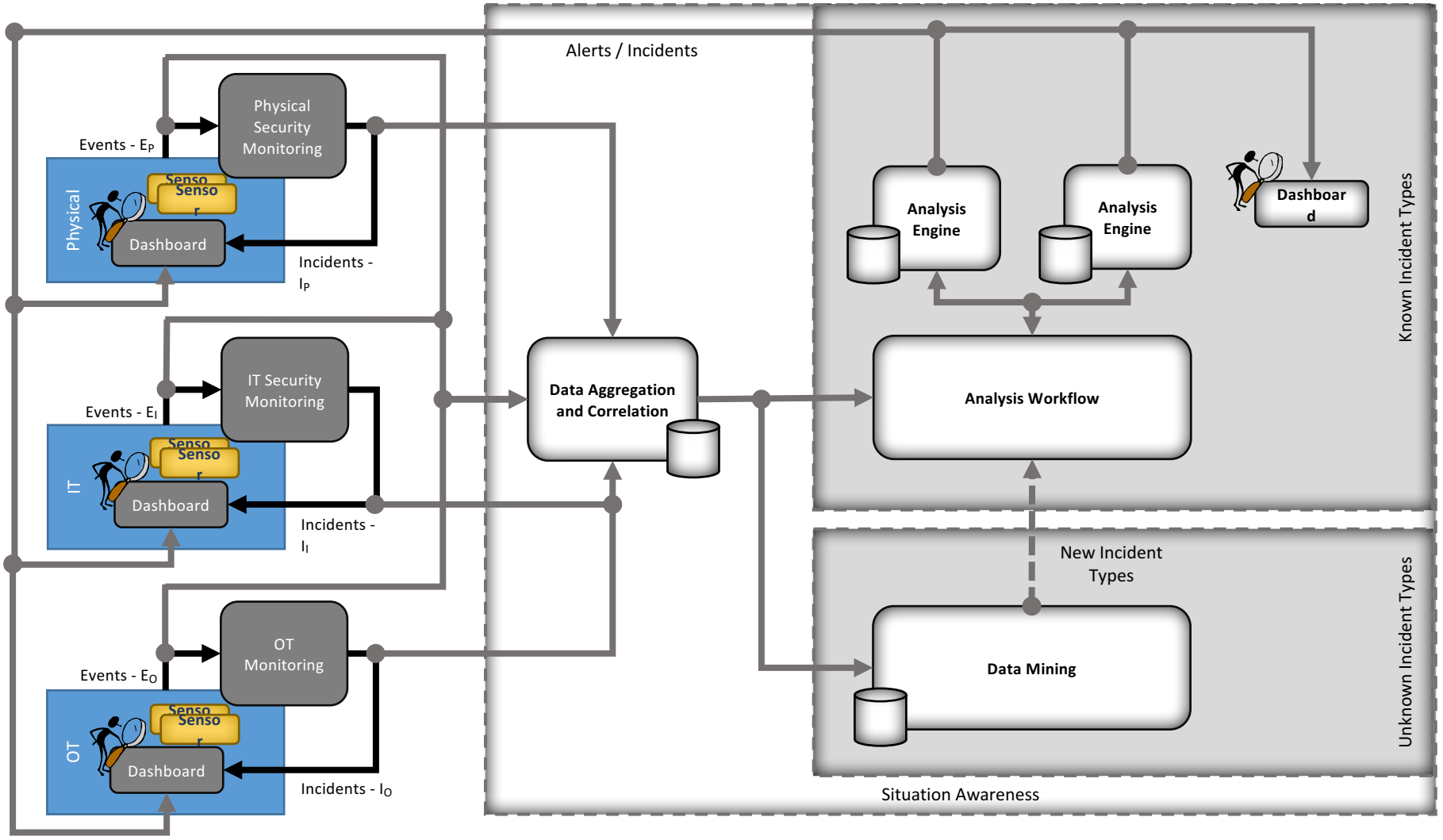
Provide information on newly-discovered incident types to analysis engines





Step Four

Augment silos with new sensor types to provide improved incident prediction / detection


Alerts / Incidents
Physical Security Monitoring
Events - E_P
Physical
Sensor
Sensor
Dashboard
Incidents - I_P
IT Security Monitoring
Events - E_I
IT
Sensor
Sensor
Dashboard
Incidents - I_I
OT Monitoring
Events - E_O
OT
Sensor
Sensor
Dashboard
Incidents - I_O
Data Aggregation and Correlation
Analysis Engine
Analysis Engine
Dashboard
Analysis Workflow
Known Incident Types
New Incident Types
Data Mining
Unknown Incident Types
Situation Awareness

Situation Awareness Project Lifecycle