Southern Company

DE-FE031640
Operational Technology Behavioral Analytics

NETL 2021 Integrated Project Review Meeting - Joint Artificial Intelligence

May 13, 2021

Clifton Black
Principal Engineer
Research & Development
Southern Company

Operational Technology Behavioral Analytics (OTBA)

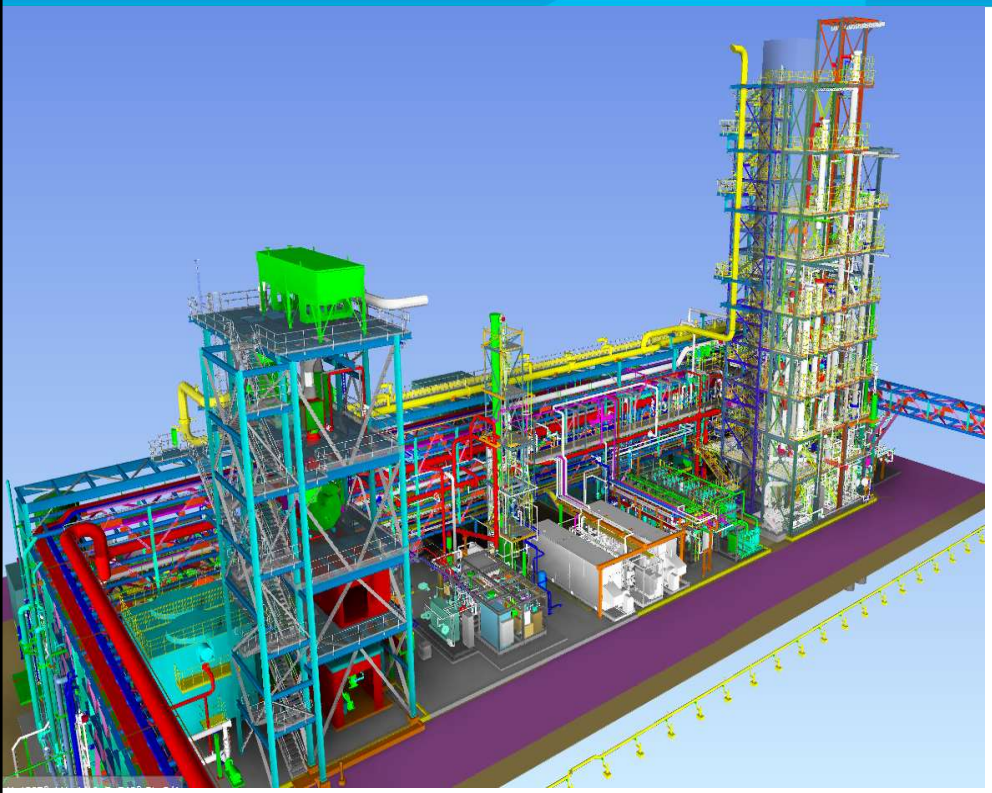
NATIONAL ENERGY TECHNOLOGY LABORATORY

Southern Company

- DE-FE00031640
- Southern Company Project Team
  - Research & Development
  - IT Security
  - NCCC
- Project Funding: $322,894
  - DOE Share - $249,985
  - Cost Share - $72,909
- Performance Period:10/1/18 – 9/30/21

Hosted at the National Carbon Capture Center

Project Objectives



Post-Combustion Carbon Capture

Reduce cyber risks in the production of energy through improved Operational Intelligence:

- *Capture machine data in an operational infrastructure*
- *Generate a high-level overview of data communications*
- *Identify normal vs abnormal behavior*
- *Develop an enhanced knowledge of risks and risk management techniques*

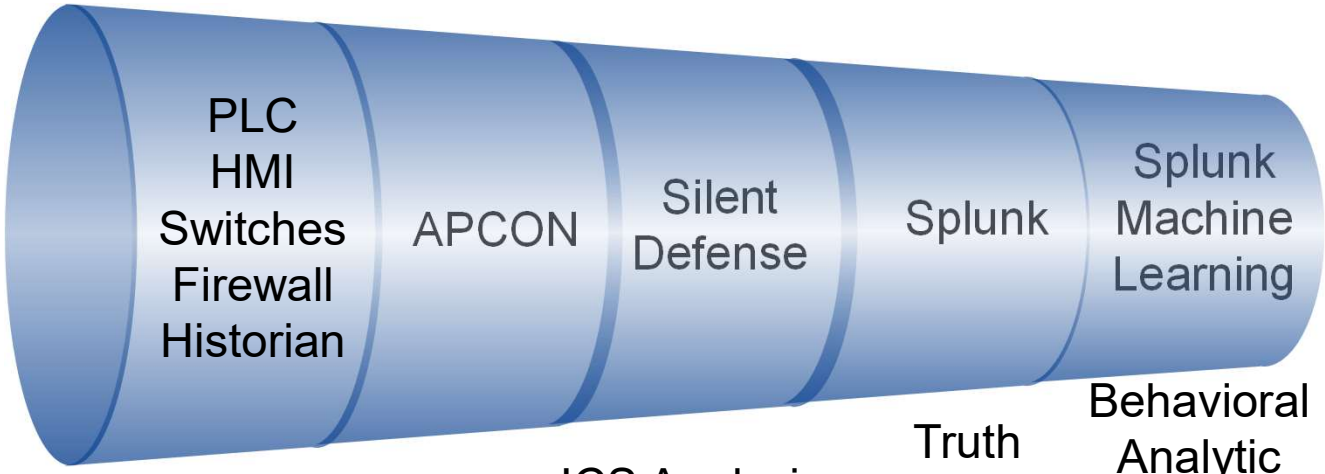
Project Overview

Task 1
Project Management

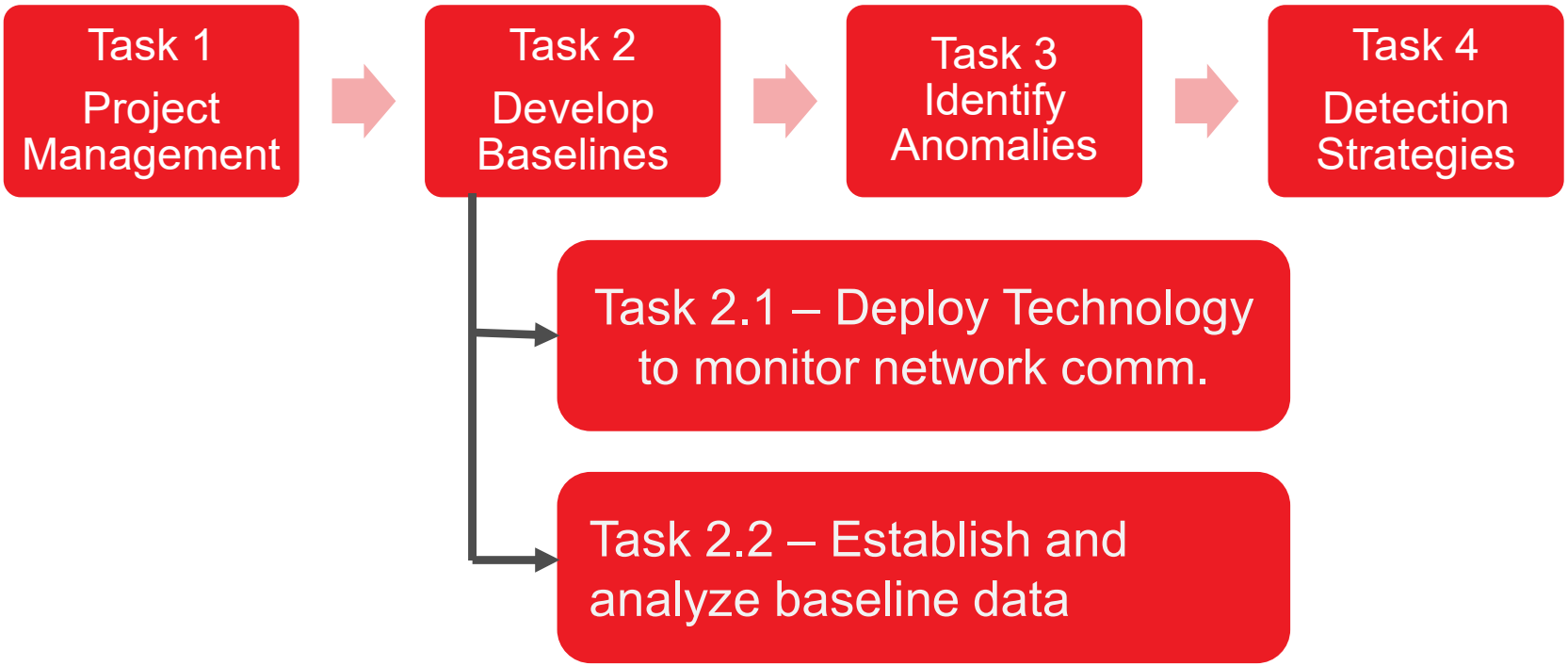
Task 2
Develop Baselines

Task 3
Identify Anomalies

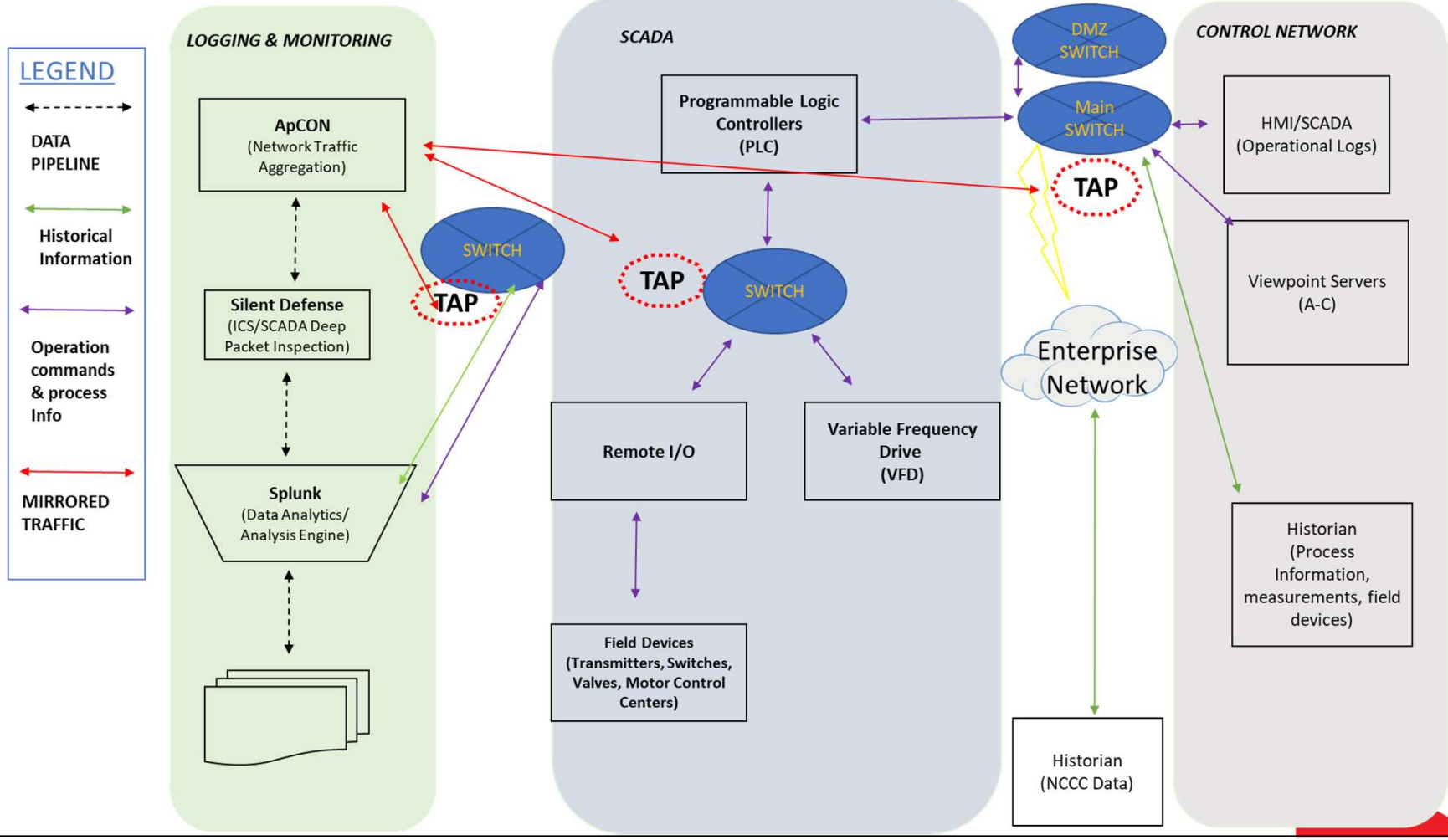
Task 4
Detection Strategies



Task 2 Updates

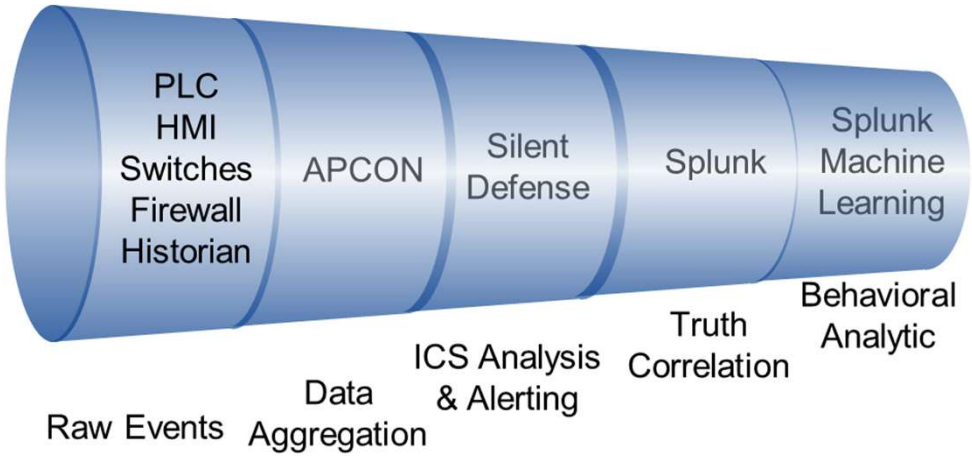


Task 2.1 – Deploy Network Monitoring Technology



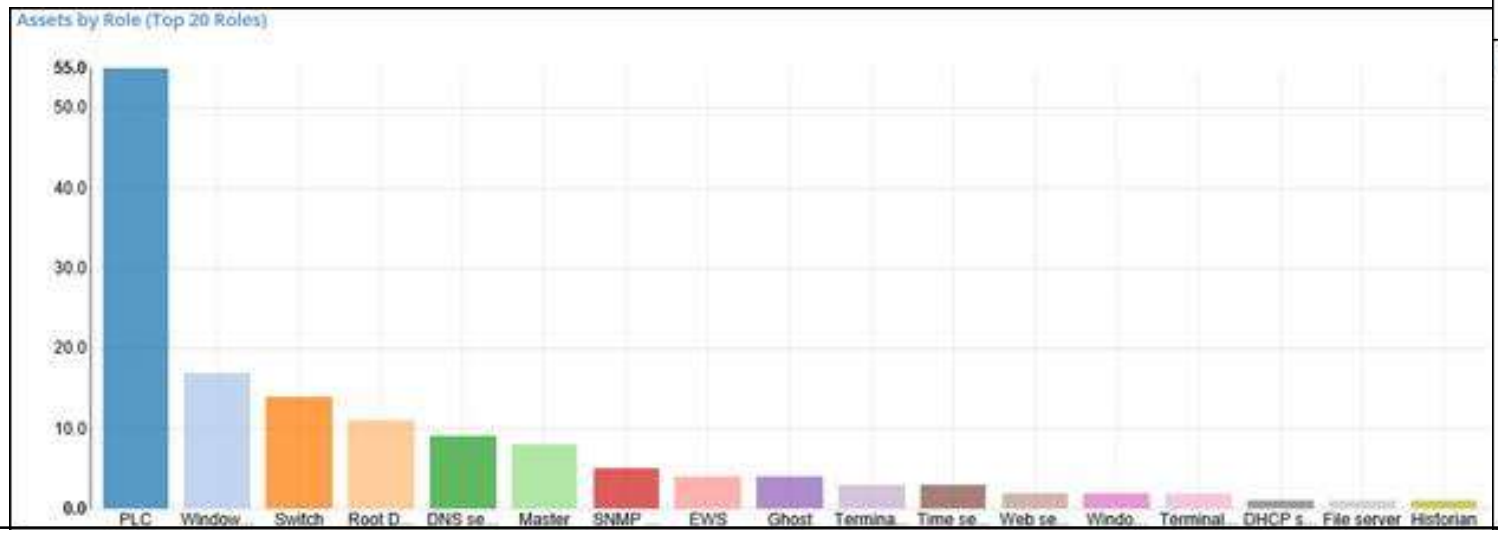
Task 2.2 – Establish Baselines (Ongoing)

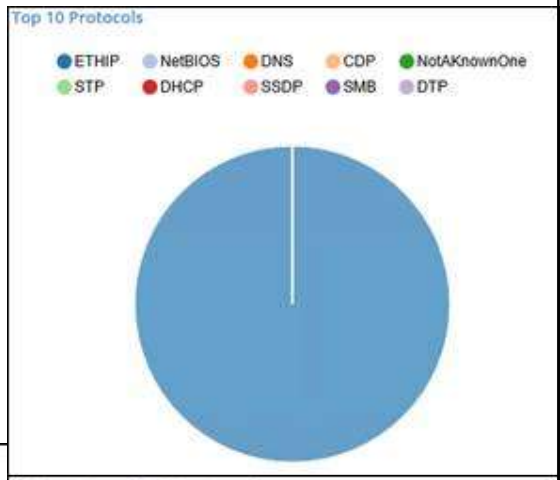
- Raw Events: event-based data from ICS, traditional network and security sources
- Data Aggregation: Raw packet capture data from multiple network switches
- ICS Analysis & Alerting: Decoding and analyzing and alerting based on raw packet capture data
- Truth Correlation: Validation of event-based and network-based data.

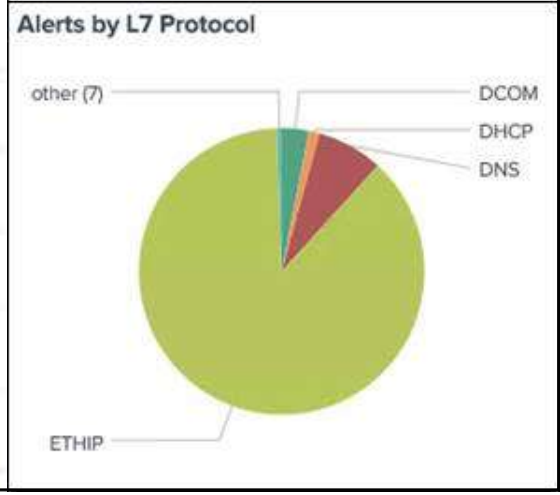


Task 2.2 – Establish/Analyze Baseline Data (Ongoing)

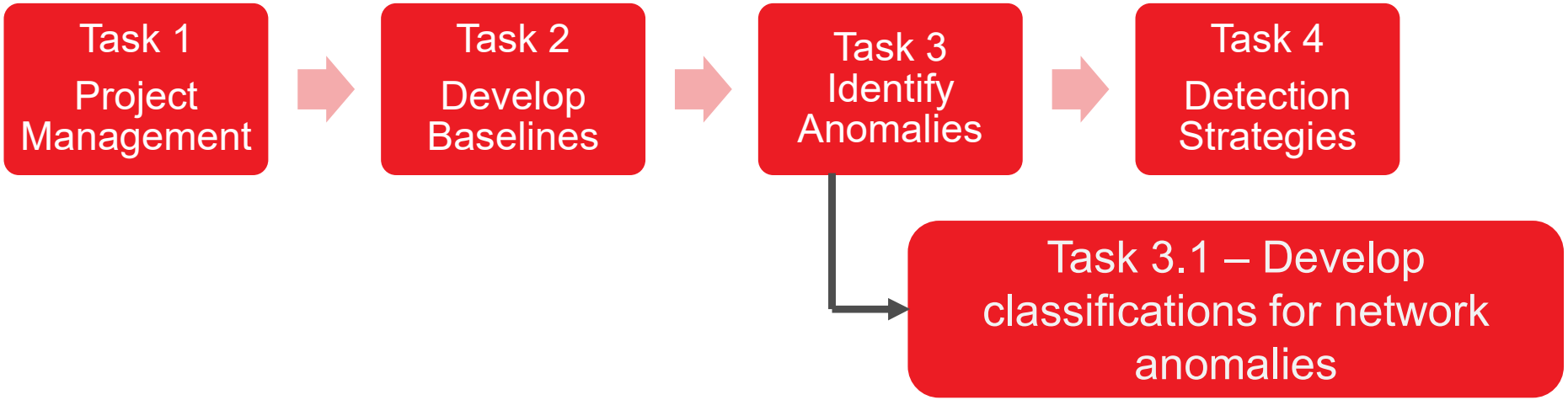
- Collection of operational data pre-COVID-19 shut down
  - Over 200 days of operational data (~ 6 months)
  - A volume of over 85 GB or raw event data
  - Observation of over 232 million total raw events
- Preliminary review of data
  - Communication between 376 NCCC network elements
  - More than 20 unique OT/ICS network device categories identified
  - Identified multiple traffic protocols



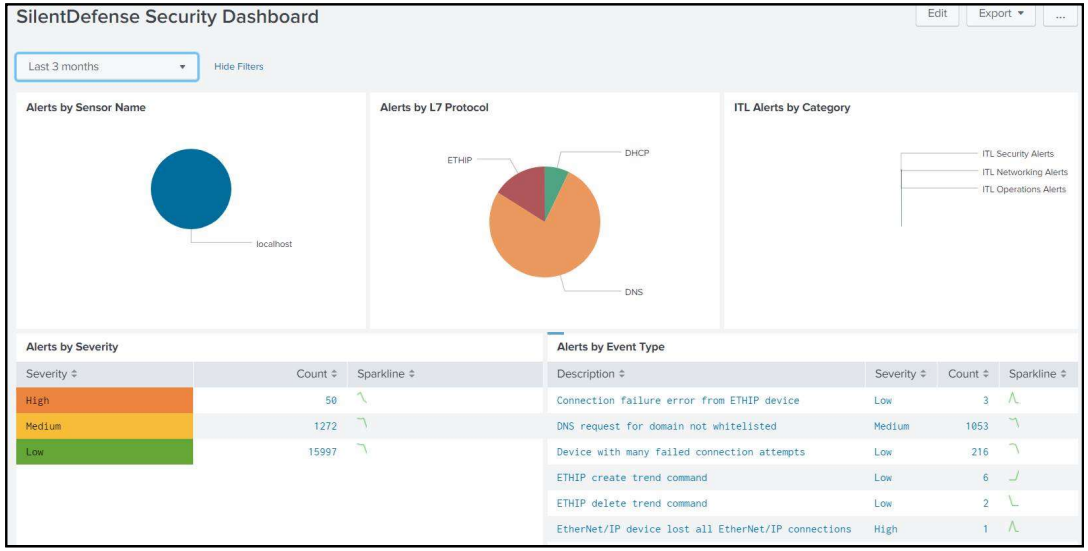




Task 3 Updates - (Ongoing)

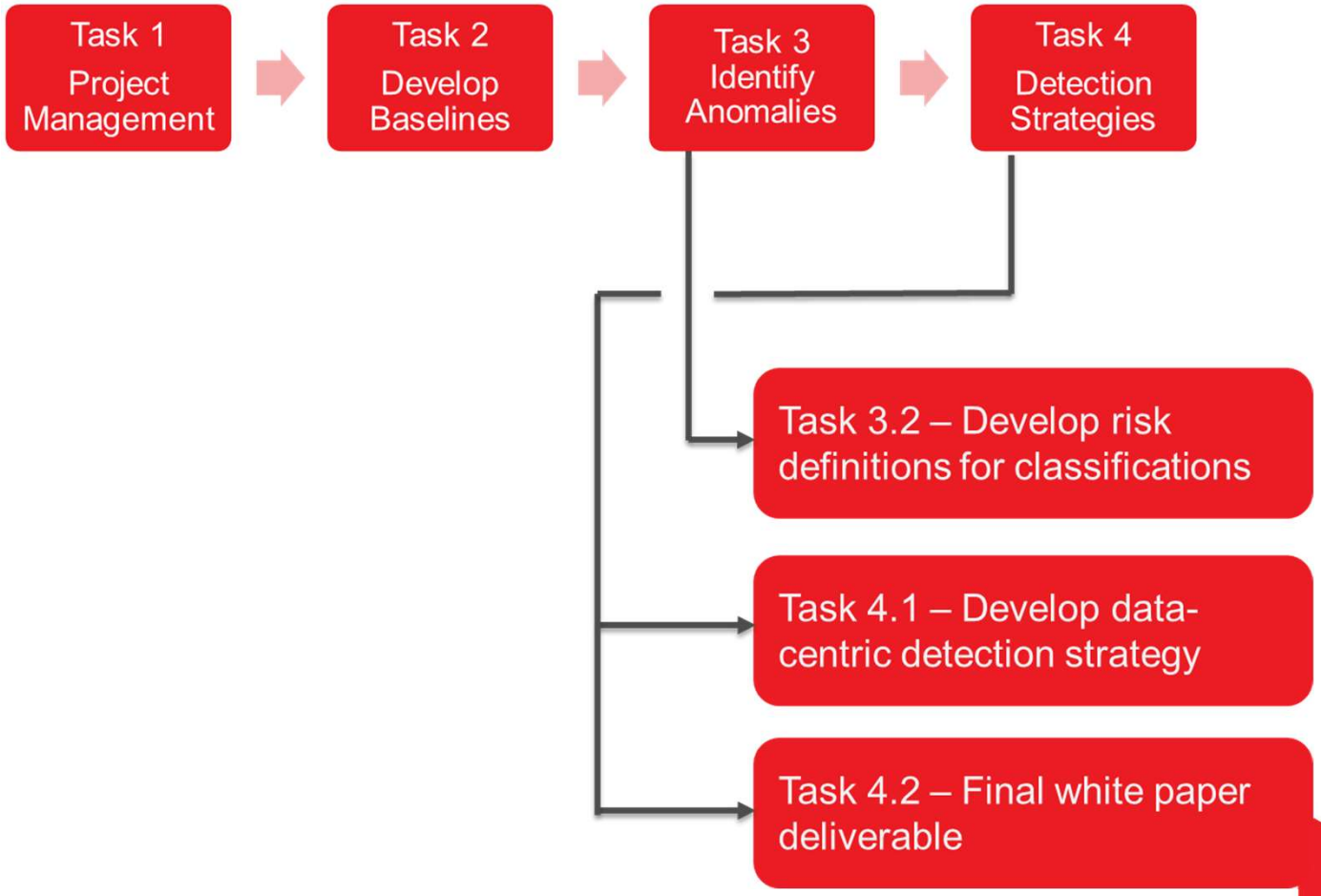


Task 3.1 – Develop classifications for network anomalies (Started)



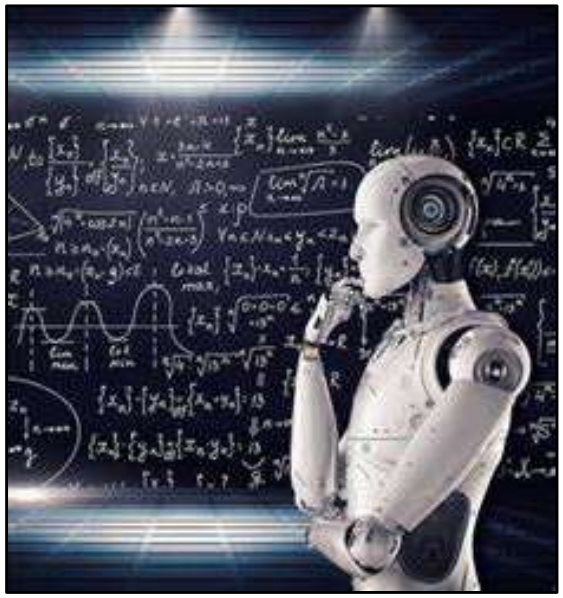
- Categorizing assets and decoding events on the network
- Correlating decoded events with raw ICS event data to classify plant operations in terms of protocol, vendor, risk, and other metrics.
- Validating data accuracy for model creation
- Analyzing results to generate insights into normal behavior and anomalies through artificial intelligence.

Next Steps – Remaining Tasks



Task 3.2 Develop Risk Definitions for Classifications

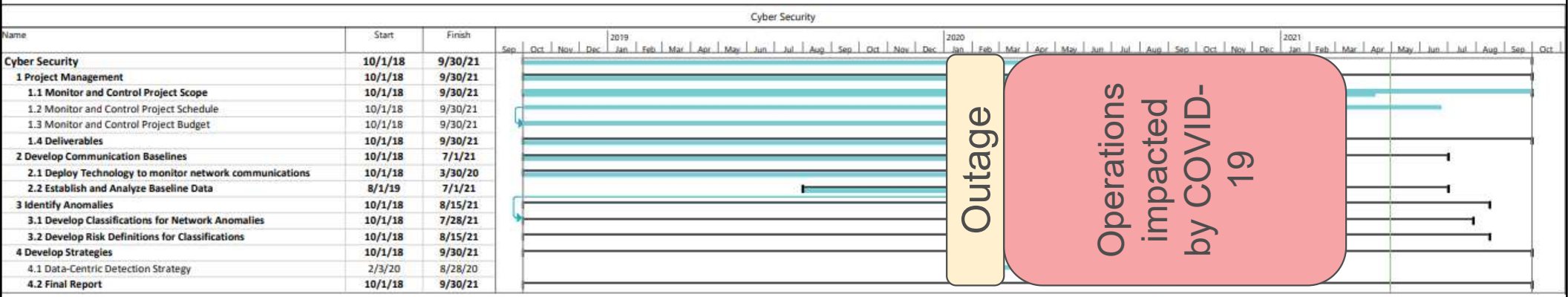
- Assess deviations from baseline to develop risk classification
  - Operator Actions
  - System Operations
- Develop risk classifications
- Assess deviations
- Characterize deviations from risk classifications
- Determine alerting strategy



Task 4.1 Develop Data Centric Detection Strategy

- Develop a model to characterize the normal behavior of an ICS environment
- Evaluate feasibility of AI-based anomaly detection method in an ICS environment which may be indicative of a cyberattack

Next Steps Contd.



Name	Start	Finish
Cyber Security	**10/1/18**	**9/30/21**
1 Project Management	**10/1/18**	**9/30/21**
1.1 Monitor and Control Project Scope	**10/1/18**	**9/30/21**
1.2 Monitor and Control Project Schedule	10/1/18	9/30/21
1.3 Monitor and Control Project Budget	10/1/18	9/30/21
1.4 Deliverables	**10/1/18**	**9/30/21**
2 Develop Communication Baselines	**10/1/18**	**7/1/21**
2.1 Deploy Technology to monitor network communications	**10/1/18**	**3/30/20**
2.2 Establish and Analyze Baseline Data	**8/1/19**	**7/1/21**
3 Identify Anomalies	**10/1/18**	**8/15/21**
3.1 Develop Classifications for Network Anomalies	**10/1/18**	**7/28/21**
3.2 Develop Risk Definitions for Classifications	**10/1/18**	**8/15/21**
4 Develop Strategies	**10/1/18**	**9/30/21**
4.1 Data-Centric Detection Strategy	2/3/20	8/28/20
4.2 Final Report	**10/1/18**	**9/30/21**

- Project Schedule
  - Plant Operations and NCCC activities recently resumed
    - Operations were halted for approximately half of 12 month no-cost extension period
  - Additional resources have been assigned to the project

Acknowledgement

Acknowledgment: "This material is based upon work supported by the Department of Energy Award Number DE-FE0031640."