Southern Company

DE-FE031640
Operating Technology Behavior Analytics

NETL Sensors and Controls Virtual Meeting

August 27, 2020

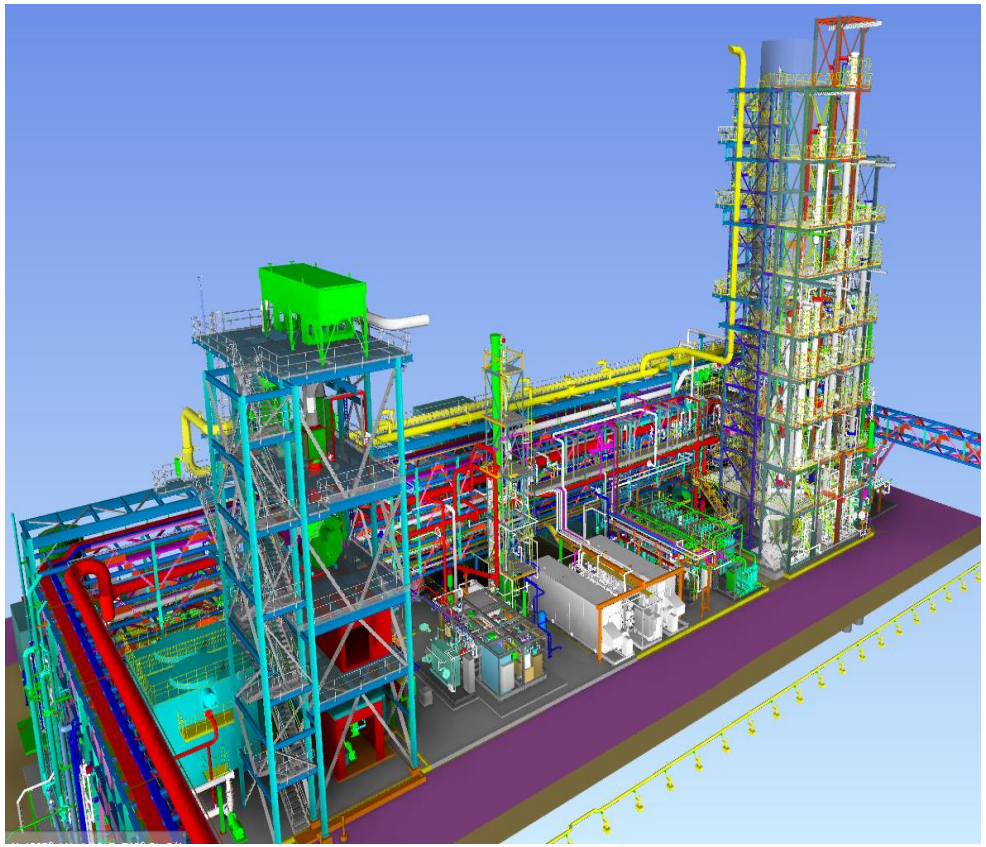
Patrick W. Crossley
Project Engineering Manager
Research & Development
Southern Company

Operational Technology Behavior Analytics (OTBA)

- 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 – 9/30/20

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*

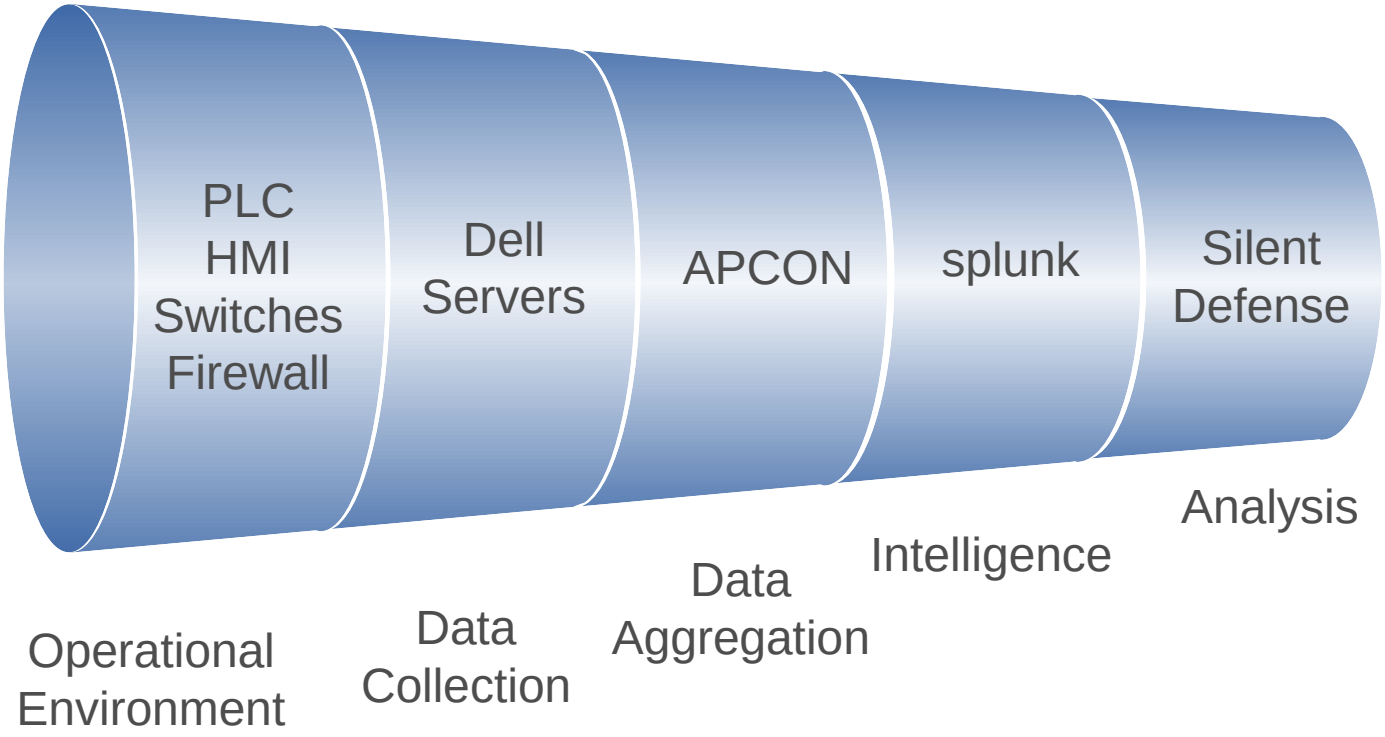
Project Overview

Task 1
Project Management

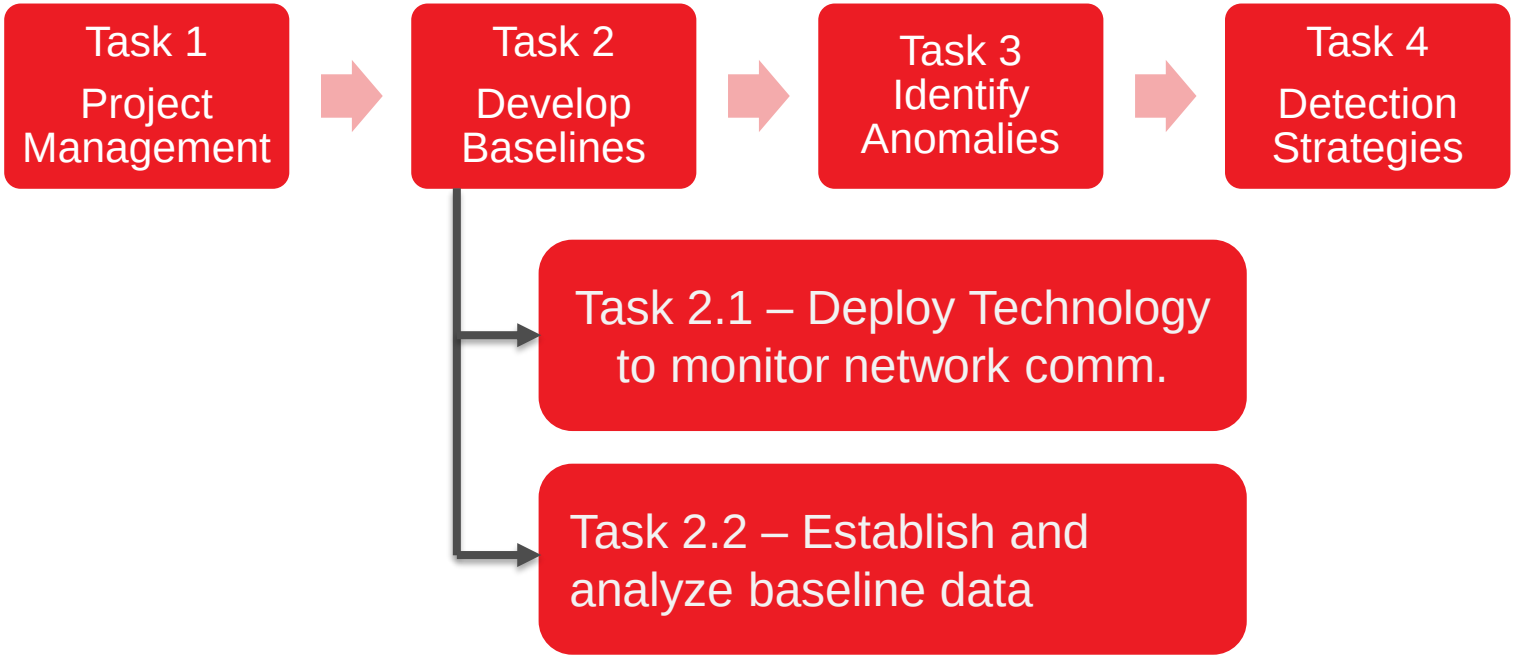
Task 2
Develop Baselines

Task 3
Identify Anomalies

Task 4
Detection Strategies

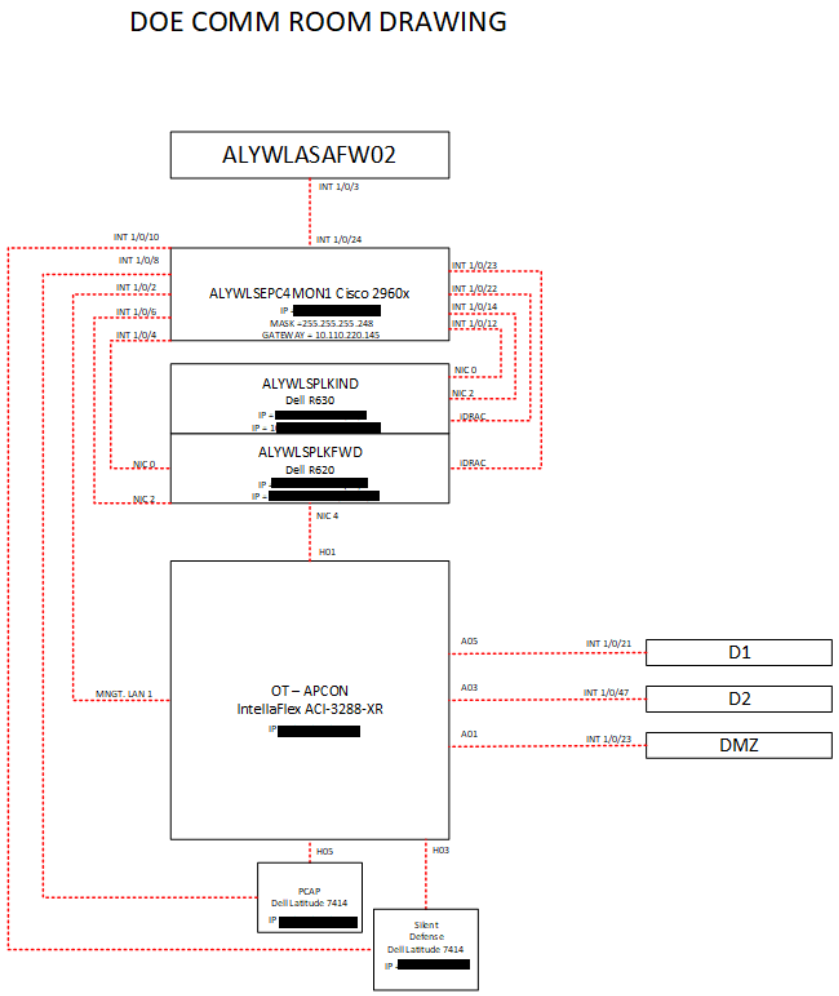


Task 2 Updates



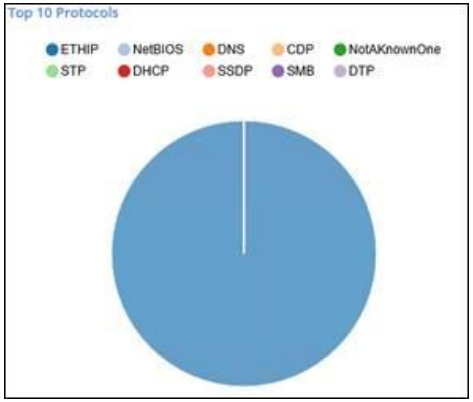
Task 2.1 – Deploy technology to monitor network data

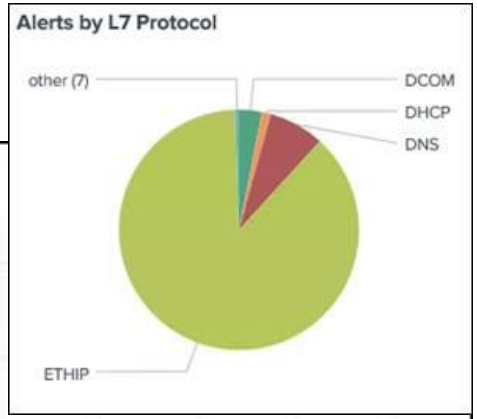
- Splunk Universal Forwarder – passive device to collect date from sources and forward RAW information
- Splunk Indexer – serves as data repository for event capture
- ApCON platform - assist in data capture from infrastructure devices.
- PCAP & Silent Defense laptops - assist with making data readable towards analyzation.
- Connected to the ICS SCADA system to review the types of high-level data that will be captured.



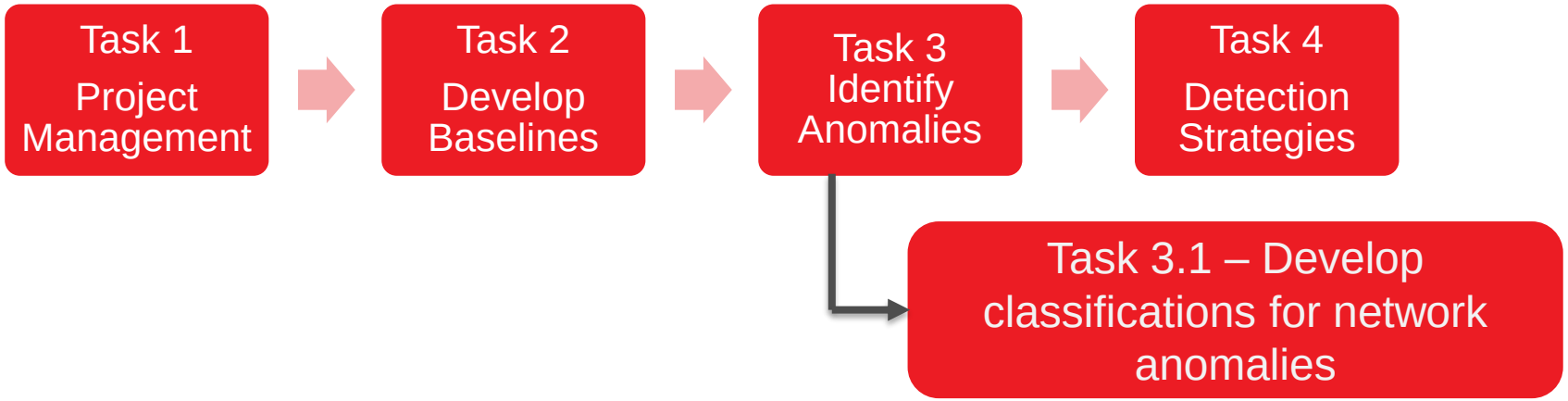
Task 2.2 – Establish/Analyze Baseline Data

- Collection of operational data
  - 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 Hosts
  - More than 20 unique OT/ICS network device categories identified
  - Identified multiple traffic protocols

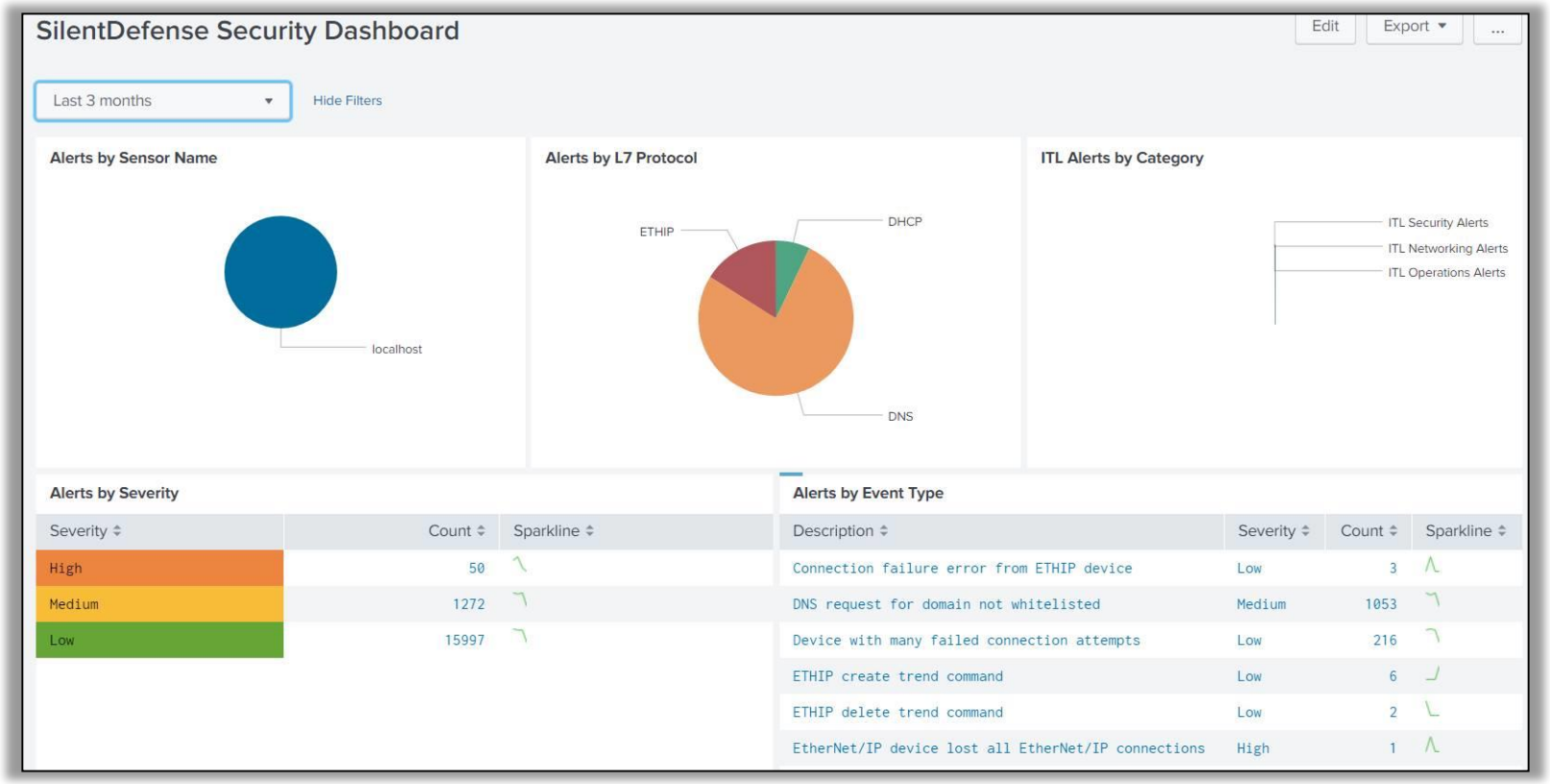




Task 3 Updates

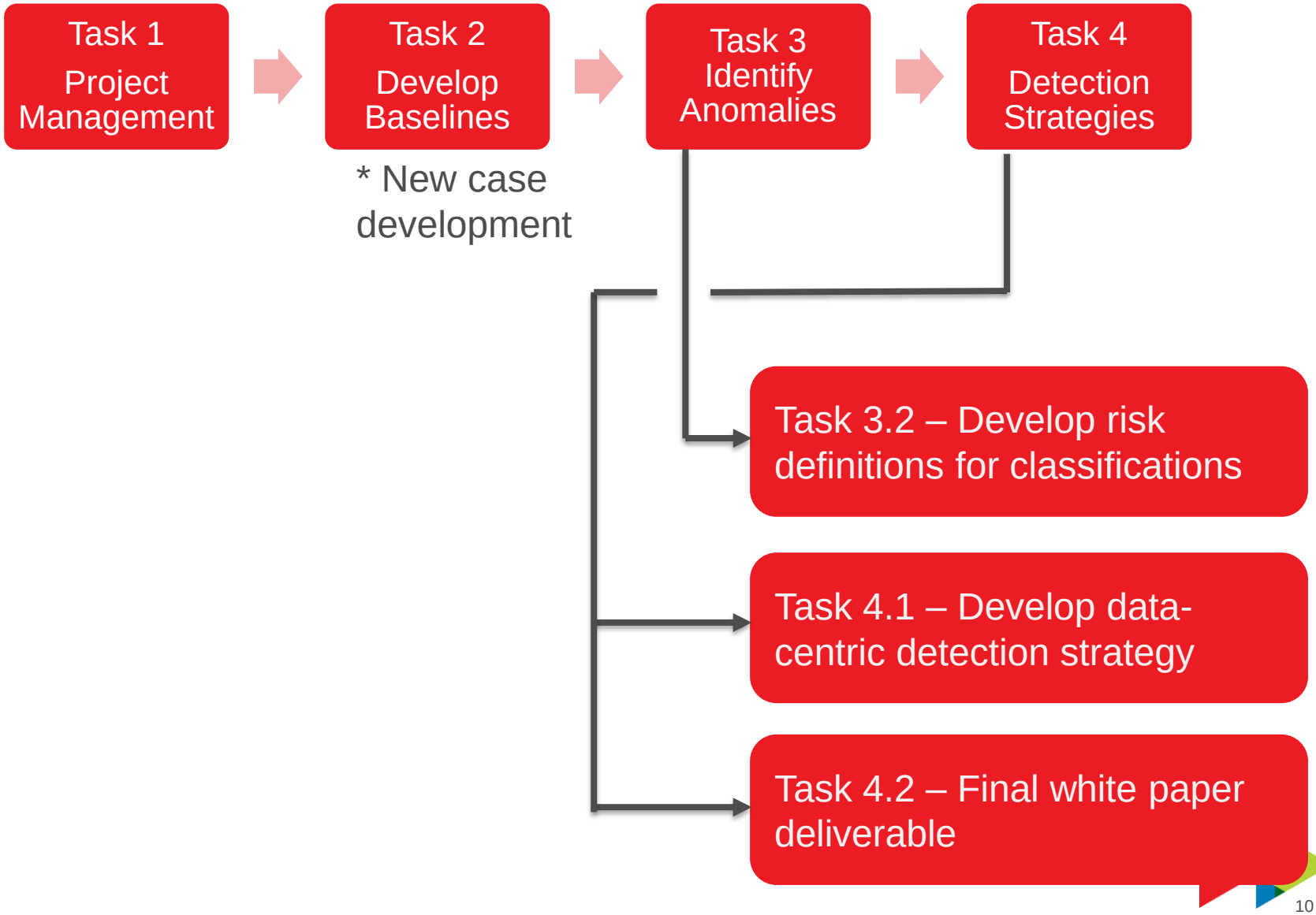


Task 3.1 – Develop classifications for network anomalies



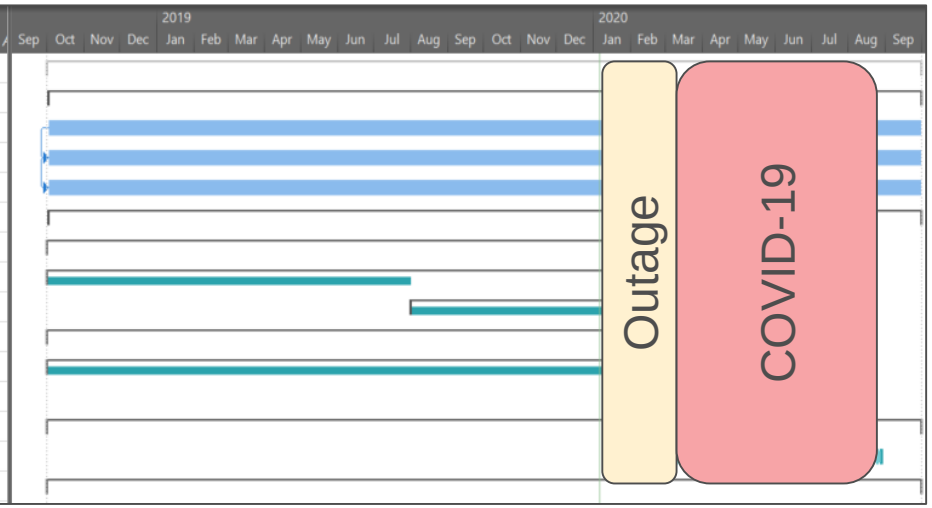
- Normalized the raw data
- System began automatically categorizing assets on the network.
- Examined the capability to classify network traffic automatically in terms of protocol, vendor, risk, and other metrics.
- Conducted analysis of ICS network traffic alert reports for activity by Severity

Next Steps – Remaining Tasks



Next Steps - Challenges

Task Name	Start	Finish
Cyber Security	**Mon 10/1/18**	**Wed 9/30/20**
1 Project Management	**Tue 10/2/18**	**Wed 9/30/20**
1.1 Monitor and Control Project Scope	Tue 10/2/18	Wed 9/30/20
1.2 Monitor and Control Project Schedule	Tue 10/2/18	Wed 9/30/20
1.3 Monitor and Control Project Budget	Tue 10/2/18	Wed 9/30/20
1.4 Deliverables	**Tue 10/2/18**	**Wed 9/30/20**
2 Develop Communication Baselines	**Mon 10/1/18**	**Mon 4/27/20**
2.1 Deploy Technology to monitor network communications	**Mon 10/1/18**	**Mon 3/30/20**
2.2 Establish and Analyze Baseline Data	**Thu 8/1/19**	**Mon 4/27/20**
3 Identify Anomalies	**Mon 10/1/18**	**Wed 5/27/20**
3.1 Develop Classifications for Network Anomalies	**Mon 10/1/18**	**Fri 2/28/20**
3.2 Develop Risk Definitions for Classifications	**Tue 5/26/20**	**Wed 5/27/20**
4 Develop Strategies	**Mon 10/1/18**	**Wed 9/30/20**
4.1 Data-Centric Detection Strategy	Mon 2/3/20	Fri 8/28/20
4.2 Final Report	**Mon 10/1/18**	**Wed 9/30/20**

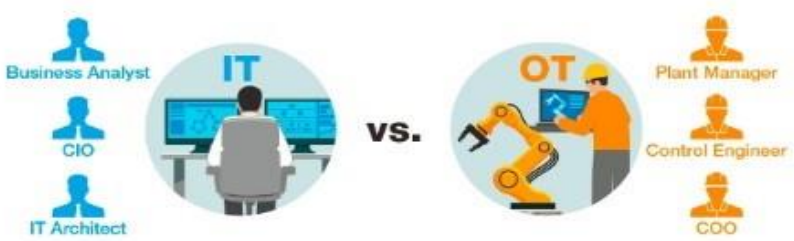


- Project Schedule
  - Submitted request to NETL for 12 month no-cost extension, extending the period of performance to 9/30/21
  - NCCC Construction activities resumed in mid-August with expectation for operations to resume in the coming months

Impact – bringing IT to OT

The top concerns for most ICS operators is SAFETY. Safety of people, damage the environment, threaten critical infrastructure. Over the last five decades, operational technology (OT) has been adopting information technology (IT) systems to improve efficiencies surrounding:

- System Health
- Configuration Management
- Continuous Monitoring
- Assessing Vulnerabilities



Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Zero downtime for control processes
Protection Targets	Windows computers, servers	Legacy industrial devices (PLC, HMI, meters)
Environmental Conditions	Air-conditioned	Harsh environments (extreme temperatures, vibrations, shocks)

Impact – Market Benefits

Characteristics		Impacts
 Alarm & Event Management		Keep systems running and reduce downtime
 Monitoring System Health		Protection from cybersecurity threats
 Troubleshooting & Investigation		Optimizing processes to reduce waste in terms of time, maintenance or product

Acknowledgements

- Sydni Credle
- Vito Cedro
- Robie Lewis

- National Carbon Capture Center


Southern Company