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
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

Operational Environment
Data Collection
Data Aggregation
Intelligence
Analysis
Silent Defense
splunk
APCON
Dell Servers
Switches
Firewall
PLC
HMI

Project Overview
Task 2 Updates

Task 1
Project Management

Task 2
Develop Baselines

Task 3
Identify Anomalies

Task 4
Detection Strategies

Task 2.1 – Deploy Technology to monitor network comm.

Task 2.2 – Establish and analyze baseline data
Task 2.1 – Deploy technology to monitor network data

- Splunk Universal Forwarder – passive device to collect data 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 1: Project Management

Task 2: Develop Baselines

Task 3: Identify Anomalies

Task 4: Detection Strategies

Task 3.1 – Develop classifications for network anomalies
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

Task 1
Project Management

Task 2
Develop Baselines

Task 3
Identify Anomalies

Task 4
Detection Strategies

* New case development

Task 3.2 – Develop risk definitions for classifications

Task 4.1 – Develop data-centric detection strategy

Task 4.2 – Final white paper deliverable
Next Steps - Challenges

• 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
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
Impact – Market Benefits

Characteristics

- Alarm & Event Management
- Monitoring System Health
- Troubleshooting & Investigation

Impacts

- Keep systems running and reduce downtime
- Protection from cybersecurity threats
- Optimizing processes to reduce waste in terms of time, maintenance or product
Acknowledgements

- Sydni Credle
- Vito Cedro
- Robie Lewis

- National Carbon Capture Center