

UNCLASSIFIED

# MOSAICS Field Test #2 Preliminary Results



18 May 2021

UNCLASSIFIED



# Agenda



- **47 CTS DT&E Overview**
- **47 CTS Field Test #2 Results**
- **346 TS Overview**
- **346 TS Practice Military Utility Assessment Results**



# 47 CTS DT&E Overview



- **Conducted 4 test events**
  - Quarterly Test December 2019
  - Field Test #1 August 2020
  - Field Test #2 (Part 1) 11-17 March 2021
  - Field Test #2 (Part 2) 3-7 May 2021
- **Test Method**
  - Initiate attacks against the MOSAICS protected ICS
  - Verify that MOSAICS correctly assess and alert
  - Verify all other MOSAICS required features
- **Summary**
  - Observed MOSAICS capability increase and objective environment integration progress



# 47 CTS Field Test #2 Results



## ■ May Results

- Six Category 2 Urgency Deficiencies
  - 3x Baselining
  - 3x SRS (User Interface)
- One Category 1 Urgency Deficiencies
  - Alerter instability

## ■ March Results (In Review)

- 10 Category 1 Urgency Deficiencies
- One Category 2 Urgency Deficiencies
- Some DRs are in review to close



# 346 TS Overview



**Test Squadron is the MAJCOM OT Org (OTO) for Cyber OT  
346 TS conducts the following spectrum of Cyber OT**

## **Military Utility Assessment (MUA)**

- Assessment of a new capability & how well it addresses military need.**
- Characterizes the military utility considering ops factors (e.g. maintainability)**

## **Force Development Evaluation (FDE)**

## **Operational Utility Evaluation (OUE)**

## **Tactics Development and Evaluation (TD&E)**

## **Operational Assessment (OA)**



# Purpose of test



**The overall purpose of the practice MUA was to conduct a dry run of MOSAICS military utility assessment (MUA).**

- **Area of focus: baselining, threat detection, and operator training**
- **Critical Operational Issue (COIs) covered:**
  - **COI 1 Will MOSAICS allow operators to detect cyber threats on ICS network?**
  - **COI 4 Can MOSAICS be sustained in its operational environment?**



# Observation



## Observations were during a dry run of MOSAICS MUA.

- The comprehensive analysis of test data may result in findings different than those presented in this briefing
- **Baseline tool:** Initial feedback from operators was mostly positive. Security and management benefits of an accurate baseline tool is invaluable to the operators
- **Threat detection:** SRS interface was intuitive but operator feedback produced additional improvements that will be provided to the developers
- **Training:** Operator training is still pending



# Baseline Tool



The screenshot displays the Baseline Tool interface within a web browser. The browser address bar shows the URL `172.20.200.114:505/Mosaics/explorer`. The interface includes a sidebar on the left with the MOSAICS logo and a navigation menu with options like 'Asset Tags', 'System Health', 'Explorer', 'Baseline Tool', and 'Maintenance List'. The main area features a 'Selection' bar at the top with a search input and a 'Retry' button. Below this is a 'Filters' section with a 'Reset All' button and a search input for filters. A 'Note-based Graph' view is active, showing a complex network graph with numerous nodes and connecting lines. The nodes are labeled with IP addresses and other identifiers. On the right side, there is a 'Nodes' panel showing a list of nodes, with one node selected: '19.200.108.14' with the agent ID 'PROCKETBEAT'. The bottom of the screenshot shows the Windows taskbar with the system clock indicating 2:11 PM on 5/16/2021.





# Questions

