



MOSAICS

MOSAICS Decision Support Needs

4 November 2020

Newton McCollum, JHU/APL



MOSAICS
2020
INDUSTRY
DAY

Unclassified Distribution A

Decision Support Overview

- The objective for MOSAICS is to monitor the facility and alert the operators and other stakeholders if there are cyber anomalies or issues within the system that require attention.



Cyber Operator – strong knowledge of the data, but may be overwhelmed with alerts



Control Systems Engineer – understands the systems but not the cyber data



Incident Response Team – deep cyber experts, but not system experts



MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A

Cyber Operator Decision Support



- Requires numerous data points to monitor the system
 - Sensors at servers / workstations, networks, relays, field device controllers
- Required to investigate alerts to determine validity
- Stand-alone sensors overload the operator with alerts from independent parts of the system
- MOSAICS needed an alert structure to incorporate various data sources and correlate outputs to present the operator with “high confidence” alerts



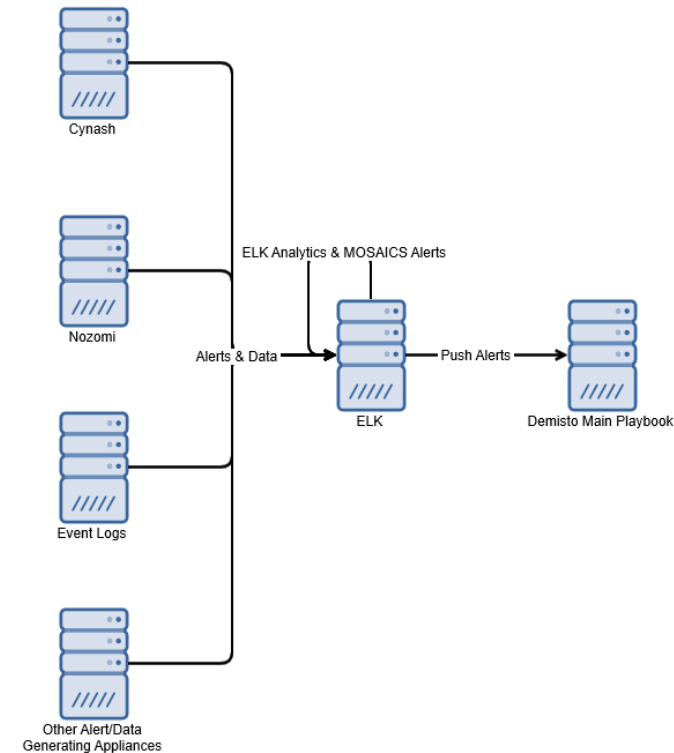
MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A

MOSAICS Alerts & Investigations

- MOSAICS Alerts – an extensible analytic architecture for receiving, correlating and aggregating alert information over time that may be related to a single attack
- Resulting Alerts are sent to Orchestrator for investigation
 - Execute associated integrity checks automatically
- Integrity checks – used to help the operator determine if a cyber event is in progress after an alert is triggered
 - Requires active collection on servers / workstations, networks devices and field device controllers





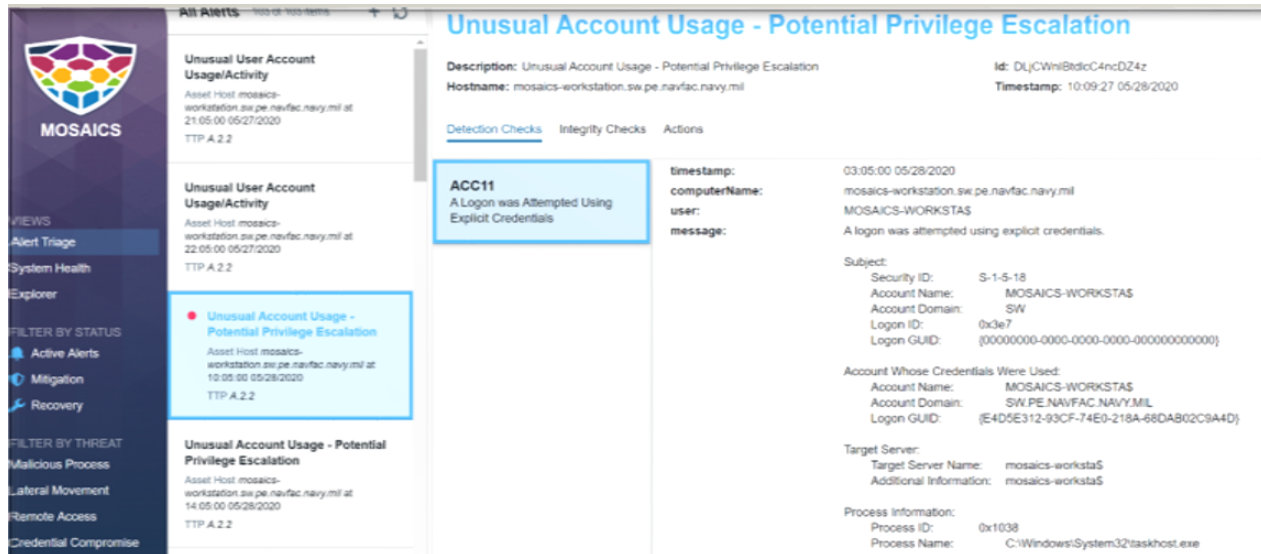
MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A

MOSAICS Alerts Outputs

1. Displayed in MOSAICS visualization capability
2. Creates incident with the ACI TTP label
 - a) Links to data associated with original event
 - b) Links to all integrity check data



The screenshot displays the MOSAICS interface. On the left is a sidebar with navigation options: Alert Triage, System Health, Explorer, Filter by Status (Active Alerts, Mitigation, Recovery), and Filter by Threat (Malicious Process, Lateral Movement, Remote Access, Credential Compromise). The main area shows a list of alerts. One alert is highlighted with a blue box: 'Unusual Account Usage - Potential Privilege Escalation' with Asset Host 'mosaics-workstation.sw.pe.navfac.navy.mil' at '10:05:00 05/28/2020' and TTP 'A.2.2'. To the right, a detailed view of this alert is shown. It includes a description, hostname, ID, and timestamp. Below this, there are tabs for 'Detection Checks', 'Integrity Checks', and 'Actions'. The 'Detection Checks' tab is active, showing a table with columns for timestamp, computerName, user, and message. The table contains one entry for 'ACC11' with a message stating 'A Logon was Attempted Using Explicit Credentials'. Below the table, there is a section for 'Account Whose Credentials Were Used' and 'Target Server' information.

3. Provides pre-approved mitigation options to the operator
4. Human decision, automated execution of mitigation decisions



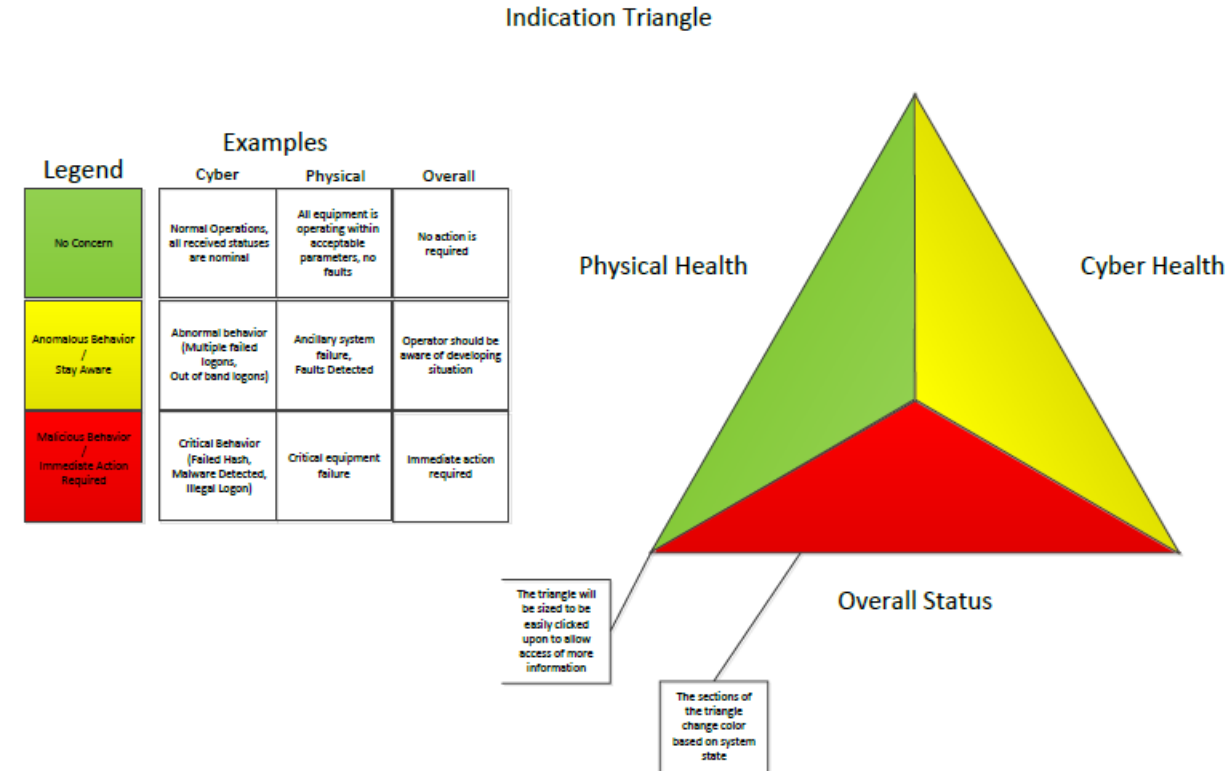
MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A

How to Assist the Control Systems Engineer

1. Cyber monitoring of key components in facility
 - a. Needs awareness on cyber aspects as they pertain to facility operations
2. Differentiate cyber effects from physical malfunction
3. Combine cyber status existing facility / physical visualizations
4. Return physical ramifications back for cyber reporting



Unclassified Distribution A

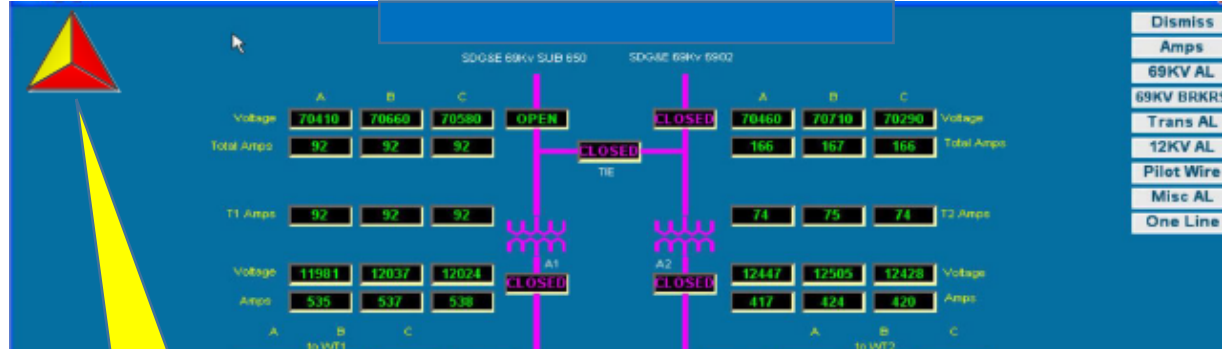


**2020
INDUSTRY
DAY**

Unclassified Distribution A

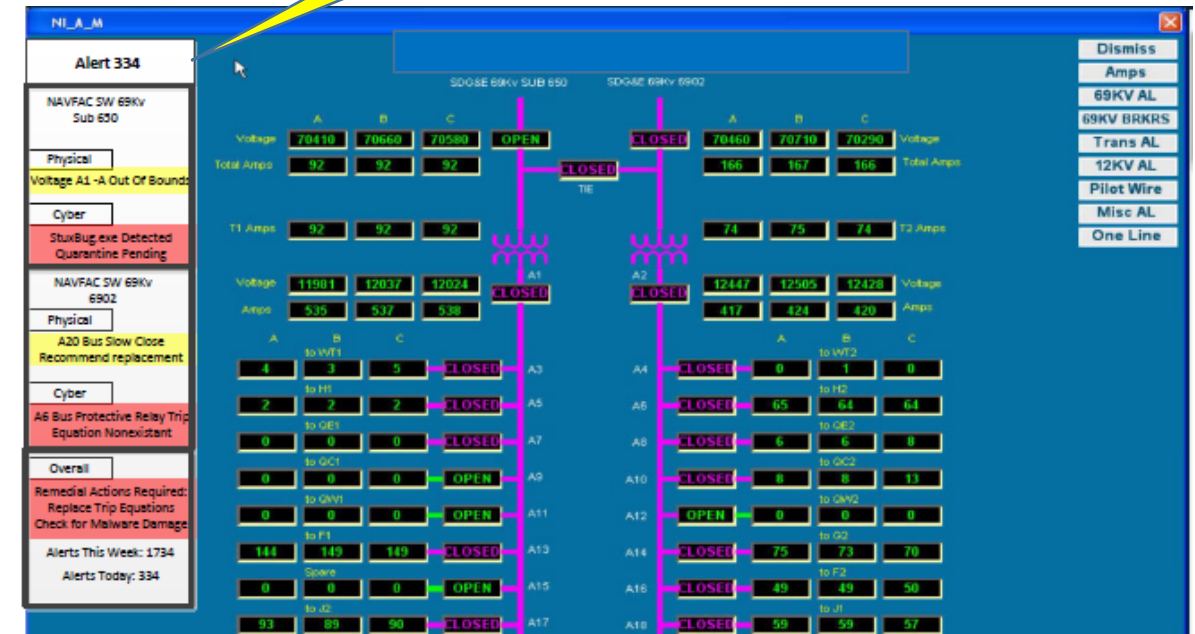


CS Exemplar Visualizations



Quick Reference Status

Detailed Status Elements



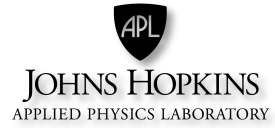
Unclassified Distribution A



MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A



How to Assist the Incident Response Team

1. Response Teams assist the facility when alerted to an incident
 - a. Arrive hours or more likely days post-incident
2. While deep cyber experts, they have limited knowledge of the control system and/or environment
3. Often lack essential data needed to determine adversary actions
 - a. Baseline data (known state)
 - b. Additional event/alert data
 - c. Deltas from baseline configurations
4. MOSAICS can provide critical insights often lost in other environments



MOSAICS

2020
INDUSTRY
DAY

Unclassified Distribution A

Industry Needs

1. Integration of various tool alerts to provide situational awareness
2. Standardization of data fields to be extracted, processed, and displayed
3. Ability to compare data across a known baseline
4. Higher level alerts based on post processing of searched data
 - a. Aggregation of results from tagged objects
5. Standardized displays to convey intuitive meaning of cyber alerts to control system operators
 - a. Visualization of the impact of events into the broader view of the facility



MOSAICS

**2020
INDUSTRY
DAY**

Unclassified Distribution A



Questions?