JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

AOS-24-0912
August 2024

# More Situational Awareness for Industrial Control Systems (MOSAICS) Block 1 Specification

DRAFT

## Version 1.0

Prepared for: Naval Facilities Engineering Systems Command (NAVFAC)

Prepared by: The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099

| | |
|---|---|
| Task No.: | CFRCS |
| Contract No.: | N00024-22-D-6404 |
| Controlled by: | NAVFAC HQ CIO |
| Distribution/Dissemination: | Approved for public release: distribution is unlimited. |
| POC: | Jacob Morris, Jacob.j.morris3.civ@us.navy.mil, (757) 637-2670 |

# CONTENTS

## FIGURES

## TABLES

# 1. INTRODUCTION

## 1.1 Background

More Situational Awareness for Industrial Control Systems (MOSAICS) is a Department of Defense (DoD) effort to modernize the detection and response to threats to Industrial Control Systems (ICS). It represents the first-ever comprehensive, integrated, and automated cyber defense capability for ICS, allowing system operators (users) to quickly, easily, and effectively detect and characterize cyberattacks in near-real time. By modeling the prescriptive approach in the DoD's Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP)[1] document and applying Information Technology (IT) automation principles, MOSAICS effectively advances the scale and speed in identifying, investigating, and responding to incidents within the ICS system.

## 1.2 Purpose and Scope

This document provides the requirements for Block 1 MOSAICS. Block 2 will be addressed in a future specification. This document covers the functional and technical MOSAICS requirements, as they apply to the system, deployment considerations and additional technical implementation details. This information is intended to be used by those deploying MOSAICS Block 1 capabilities to assist in identifying compatible technical solutions and integrating those solutions into a viable MOSAICS implementation. This is a living document that will be supplemented with additional information in the future.

[1] https://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS_Rev_2_(Final).pdf

# 2. MOSAICS OVERVIEW

## 2.1 MOSAICS Framework Overview

MOSAICS provides a framework that defines a body of functions and requirements for control system cyber threat defense organized into blocks. MOSAICS Block 1 allows organizations to achieve continuous passive and safe active monitoring of control system network assets. MOSAICS provides a single data repository for continuous collection of host event data, network intrusion detection alerts, network equipment logs, and network flow metrics for performing correlative analytics. MOSAICS Block 1 provides basic workflow management (See Appendix A for details) of a system baseline and on-demand integrity checking of control system assets against a stored system baseline. The MOSAICS framework has the following characteristics:

- Vendor-agnostic architecture
- Behavior-based correlative analytics
- Intelligent automation
- Operator (user)-focused cyber visualizations
- Automated information sharing

## 2.2 Block and Sub-Block Definitions

A MOSAICS capability is an implemented instantiation of the MOSAICS framework. MOSAICS capabilities are presented in terms of Blocks and Sub-blocks (Table 2-1).

**Table 2-1 MOSAICS Blocks and Sub-blocks**

| Block | Sub-Block | Description | Capabilities |
|---|---|---|---|
| 1 | A* | Continuous passive monitoring of control system network and assets into a single data repository performing correlative analytics. Continuous collection of host event data, network intrusion detection alerts, network equipment logs, and network flow metrics. | - Host monitoring<br>- Network monitoring<br>- Single aggregated event data repository<br>- Behavioral aggregation analytics<br>- Behavioral set correlation analytics<br>- Visualization of events, behaviors, and alerts |
| 1 | B* | Includes all functionality from Block 1A. Safe active enumeration of control system network and assets. Basic workflow management of a system baseline and on-demand integrity checking of control system assets against stored system baseline. | - All Block 1A Capabilities<br>- Active enumeration of network equipment<br>- Integrated system baseline creation<br>- Workflow management for baseline creation and alert investigation<br>- Host investigation with integrity checks |

| Block | Sub-Block | Description | Capabilities |
|---|---|---|---|
| 2 | A | Includes all functionality from Block 1B. SOAR management of a system baseline and on-demand integrity checking of control system assets against stored system baseline. Automated generation of recommended courses of action, with SOAR automated execution of user-selected mitigations. | - All Block 1B Capabilities<br>- SOAR automation for course-of-action suggestion<br>- User-selected mitigation<br>- Automated execution of user-selected mitigation actions |
| 2 | B | Includes all functionality from Block 2A. Bi-directional threat intelligence sharing between MOSAICS systems. | - All Block 2A Capabilities<br>- Automated sharing of incident and mitigation details<br>- Automated consumption and use of threat intelligence data |
| 2 | C | All functionality from Block 2B. Fine-grained response actions with follow-up recovery actions. | - All Block 2B Capabilities<br>- Automated implementation of granular response actions<br>- Automated execution of recovery actions |

*Covered in this document
SOAR: Security Orchestration and Automated Response

## 2.3 Functions and Block Alignment

The MOSAICS requirements were developed around seven functional capabilities: detection, analysis, visualization, decision-making, mitigation, recovery, and information sharing (Figure 2-1).

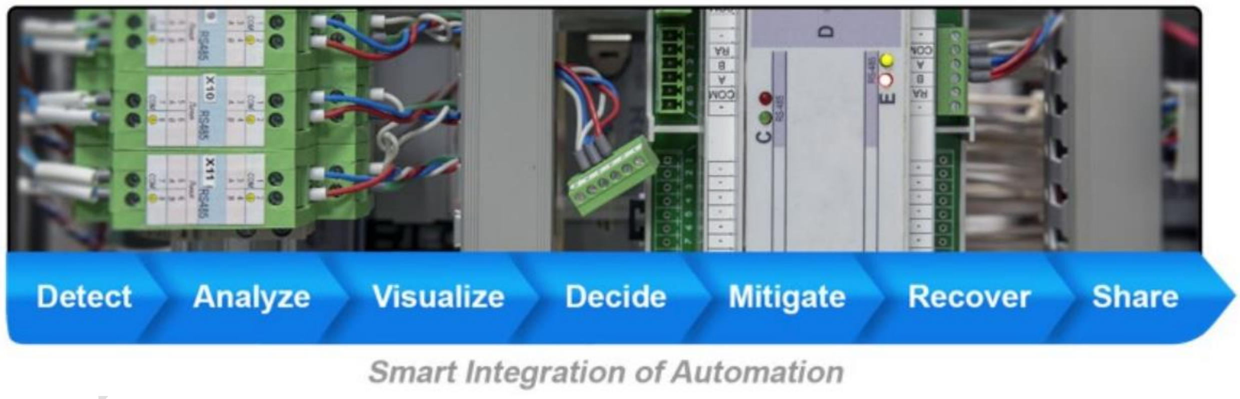


**Figure 2-1 MOSAICS Functional Capabilities**

The MOSAICS functions are shown in Table 2-2 with the associated functional capability and Block(s) in which each function is implemented. Block 1A and 1B requirements are provided in Section 4, with the block number for each individual requirement. Block 2 requirements, and future requirements in development, will be included in a future specification.

**Table 2-2 MOSAICS Functions, Functional Capabilities, and Blocks**

| MOSAICS Function | Functional Capability** | Block 1A | Block 1B | Block 2A | Block 2B |
|---|---|---|---|---|---|
| **MOSAICS System Identification*** | Detect | | | | |
| Detect and Collect Asset Information | | x | | | |
| Assign Asset Criticality | | x | | | |
| Maintain Inventory | | x | | | |
| Create Baselines | | x | | | |
| **MOSAICS System Protection** | Protect*** | | | | |
| Identity and Access Management | | x | | | |
| Data Security | | x | | | |
| Audit Logging | | x | | | |
| **MOSAICS Monitor and Detection** | Detect | | | | |
| Continuous Monitoring | | x | | | |
| Detection | | x | | | |
| Event Generation | | x | | | |
| **MOSAICS Analysis** | Analyze | | | | |
| Analyze Events | | x | | | |
| Perform Integrity Checks | | | x | | |
| **MOSAICS Visualization*** | Visualize | | | | |
| Detected Event Visualization | | x | | x | |
| Protected Enclave Status Visualization | | x | | | |
| Alert Visualization and Management | | x | x | x | |
| Orchestration and Metric Visualization | | | x | | |
| **MOSAICS Decision** | Decide | | | | |
| Event / Incident Response Analysis | | | | x | |
| **MOSAICS Mitigation** | Mitigate | | | | |
| Event / Incident Response Execution | | | | x | |
| Implement ACI TTP | | | | x | |
| **MOSAICS Recovery** | Recover | | | | |
| Recovery Planning | | | | | x |
| Recovery Forensic | | | | | x |
| Recovery Execution | | | | | x |
| Recovery Verification | | | | | x |
| **MOSAICS Information Sharing** | Share | | | | |
| Event / Incident Communication | | | | x | |
| Threat Information Communication | | | | | x |
| Facility ICS / MOSAICS Status Communication | | | | x | |

*The majority of the requirements are Block 1 and are therefore covered in this document. There are additional requirements in Block 2.

**See Figure 2-1.

*** These are protection requirements for MOSAICS and the control system data residing within MOSAICS.

# 3. MOSAICS BLOCK 1 SYSTEM OVERVIEW

A brief description of MOSAICS Block 1 functions is provided in Table 3-1, and a functional block diagram is shown in Figure 3-1.

**Table 3-1 MOSAICS Function Descriptions**

| | |
|---|---|
| System Identification Requirements | Identifies assets on the network using passive network monitoring and safe active device interrogation. Maintains asset inventories. Creates baselines used in the Analysis function. |
| System Protection Requirements | Provides access management, data security, and audit logging for MOSAICS. |
| Monitor & Detection Requirements | Monitors the assets and network behavior and detects anomalous component and communication status and activity. |
| Analysis Requirements | Correlates events, generates alerts, and performs integrity checks. |
| Visualization Requirements | Provides for visualization of events, alerts, and management of alerts, as well as display of orchestrator metrics. |

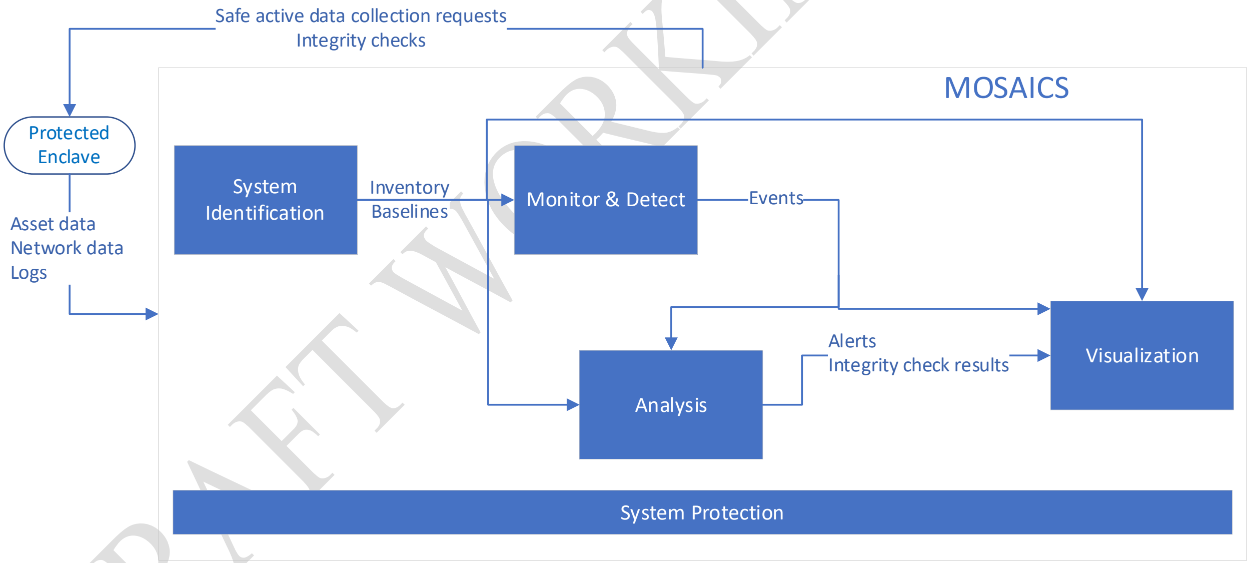
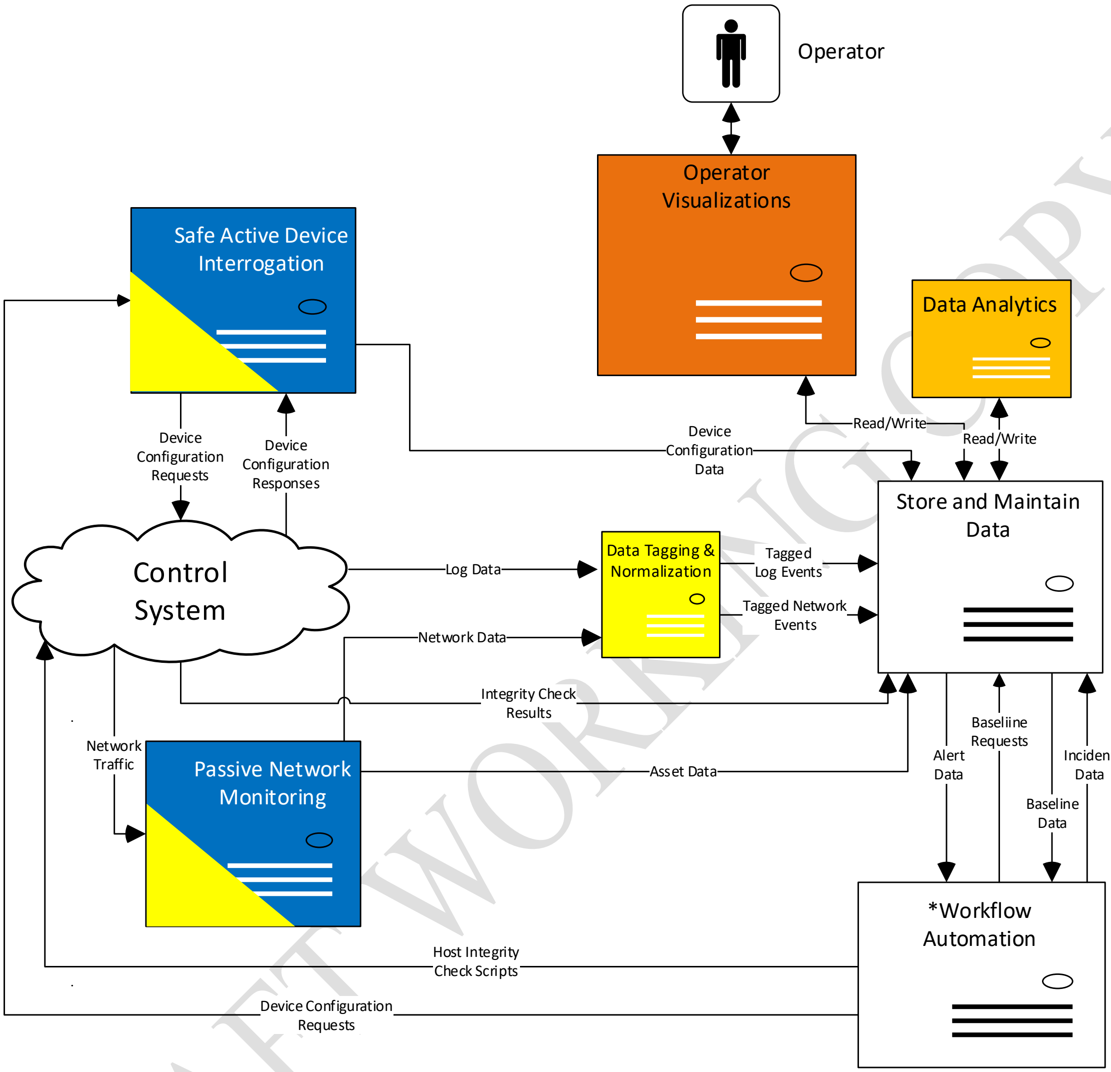


**Figure 3-1 MOSAICS Functional Block Diagram**

## 3.1 Function Descriptions

**Each function is described in further detail in this section. Key concepts, noted in bold in the function descriptions, are included in the MOSAICS reference architecture in Section 3.2,**



*Store and Maintain Data and Workflow Automation cross all Block 1 functions

Figure 3-7.

### 3.1.1 System Identification

Block 1 MOSAICS System Identification (F1.0) sub-functions are shown in Figure 3-2. Assets are detected on the network and information about them is collected (F1.1). The detection and collection of information is performed through **Passive Network Monitoring** and **Safe Active Device Interrogation.** The user may assign criticality to the asset (F1.2). Inventories of the control equipment, hosts, and network equipment are maintained (F1.3). Baselines are created for use in the Analysis function to perform integrity checks (F1.4).

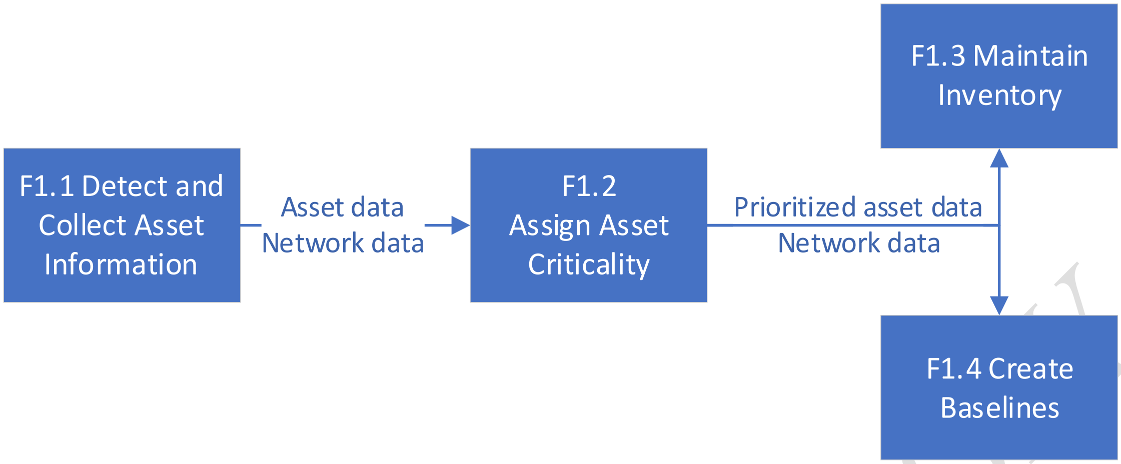


**Figure 3-2 MOSAICS Block 1 System Identification Functional Block Diagram**

### 3.1.2 System Protection Requirements

System Protection involves the protection of MOSAICS itself, rather than the protected enclave assets. MOSAICS Block 1 System Protection (F2.0) sub-functions are shown in Figure 3-3. MOSAICS obtains user information from facility authoritative sources and uses that information to provide access control. MOSAICS protects control system data contained within MOSAICS through encryption while at rest and in transit. MOSAICS generates audit logs for MOSAICS activities.

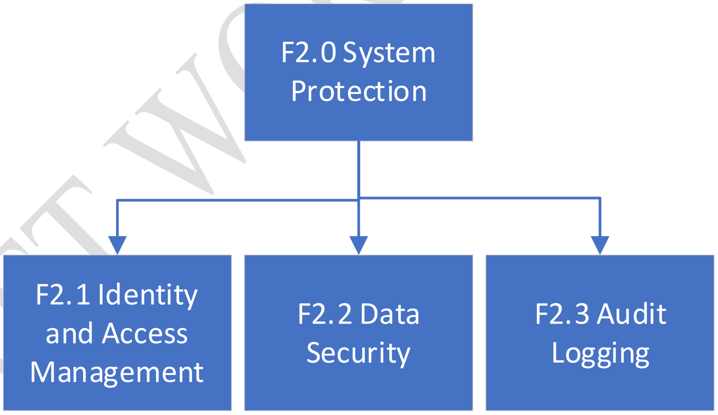


**Figure 3-3 MOSAICS Block 1 System Protection Functional Block Diagram**

### 3.1.3 Monitor & Detection Requirements

Block I MOSAICS Monitor and Detection (F3.0) sub-functions are shown in Figure 3-4. MOSAICS monitors the network communications and status of protected enclave assets and the accesses of facility protective enclave assets and systems (F3.1). MOSAICS detects changes from the baseline inventory of protective enclave assets and abnormal component behavior (F3.2), generating an event whenever any detection criteria is triggered (F3.3). This function performs **Data Tagging & Normalization**.

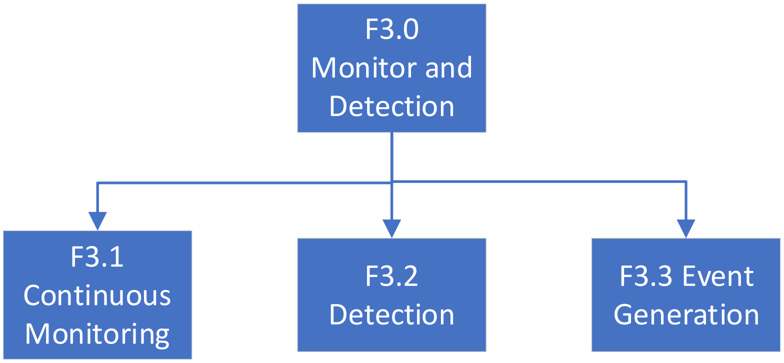


**Figure 3-4 MOSAICS Block 1 Monitor and Detection Functional Block Diagram**

### 3.1.4 Analysis Requirements

Block 1 MOSAICS Analysis (F4.0) sub-functions (**Data Analytics),** are shown in Figure 3-5. Analyze Events (F4.1) includes correlating events, assigning severity levels, and generating alerts that include relevant related information. Integrity checks, which compare the current state with the baseline, are also performed for each alert (F4.2). Appendix B details the Behavioral Alerting Sets for Control Systems (BAS/CS™), a Johns Hopkins University Applied Physics Laboratory (JHU/APL) Alerting Framework. An implementation of BAS/CS™ is one approach toward satisfying the MOSAICS alerting requirements. Other approaches that meet the requirements are acceptable.

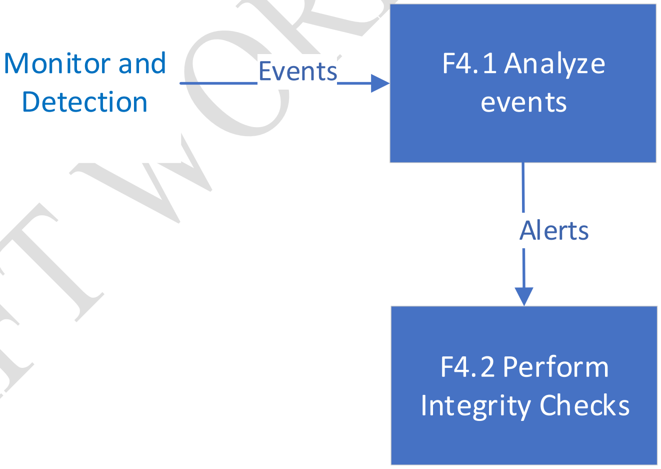


**Figure 3-5 MOSAICS Block 1 Analysis Functional Block Diagram**

### 3.1.5 Visualization

MOSAICS Block I Visualization (F5.0) sub-functions are shown in **Error! Reference source not found.** MOSAICS visualizations are a core component of providing situational awareness to the operators so they can take the most informed corrective actions based on the correlative analytics of the alerts and incidents. MOSAICS accomplishes this through a three-pronged approach. It first provides means to visualize events (F5.1). Then, MOSAICS is able to provide visualizations for the impact of these events on the protected enclave status (F5.2). Finally, MOSAICS provides alert visualizations, alert management features for alert acknowledgement, and alert assignment in the case of a team working to resolve any incidents (F5.3). MOSAICS also provides visualizations displaying the metrics for the orchestrator and playbook time to completion in order for the operator to understand how long these processes are taking (F5.4). Appendix C provides example screenshots for the implementation of MOSAICS visualization requirements.

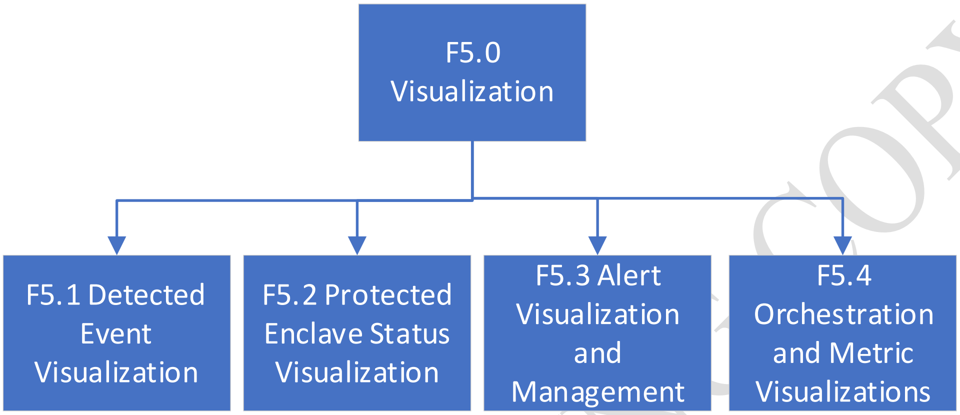
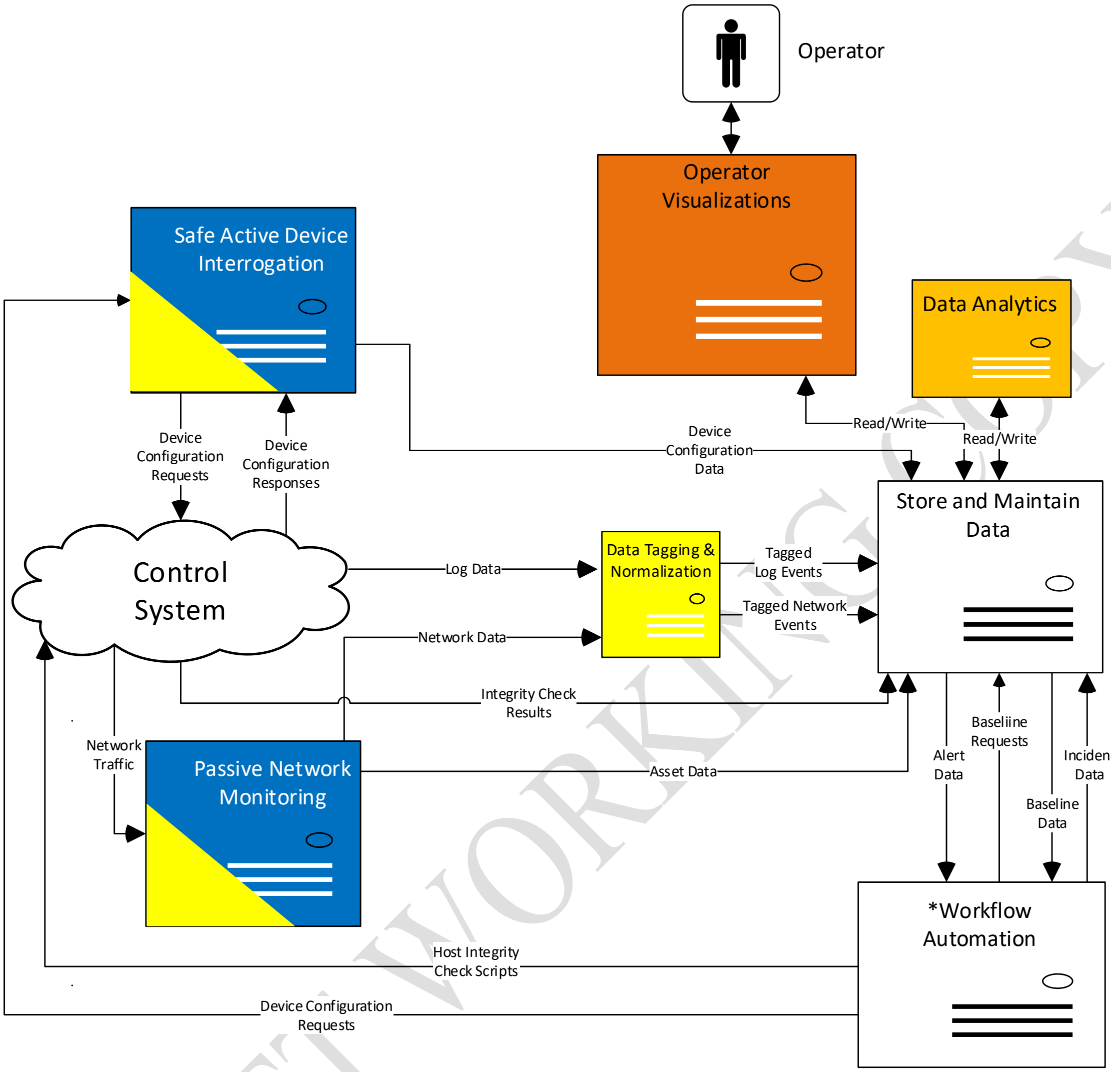

F5.0 Visualization
F5.1 Detected Event Visualization
F5.2 Protected Enclave Status Visualization
F5.3 Alert Visualization and Management
F5.4 Orchestration and Metric Visualizations

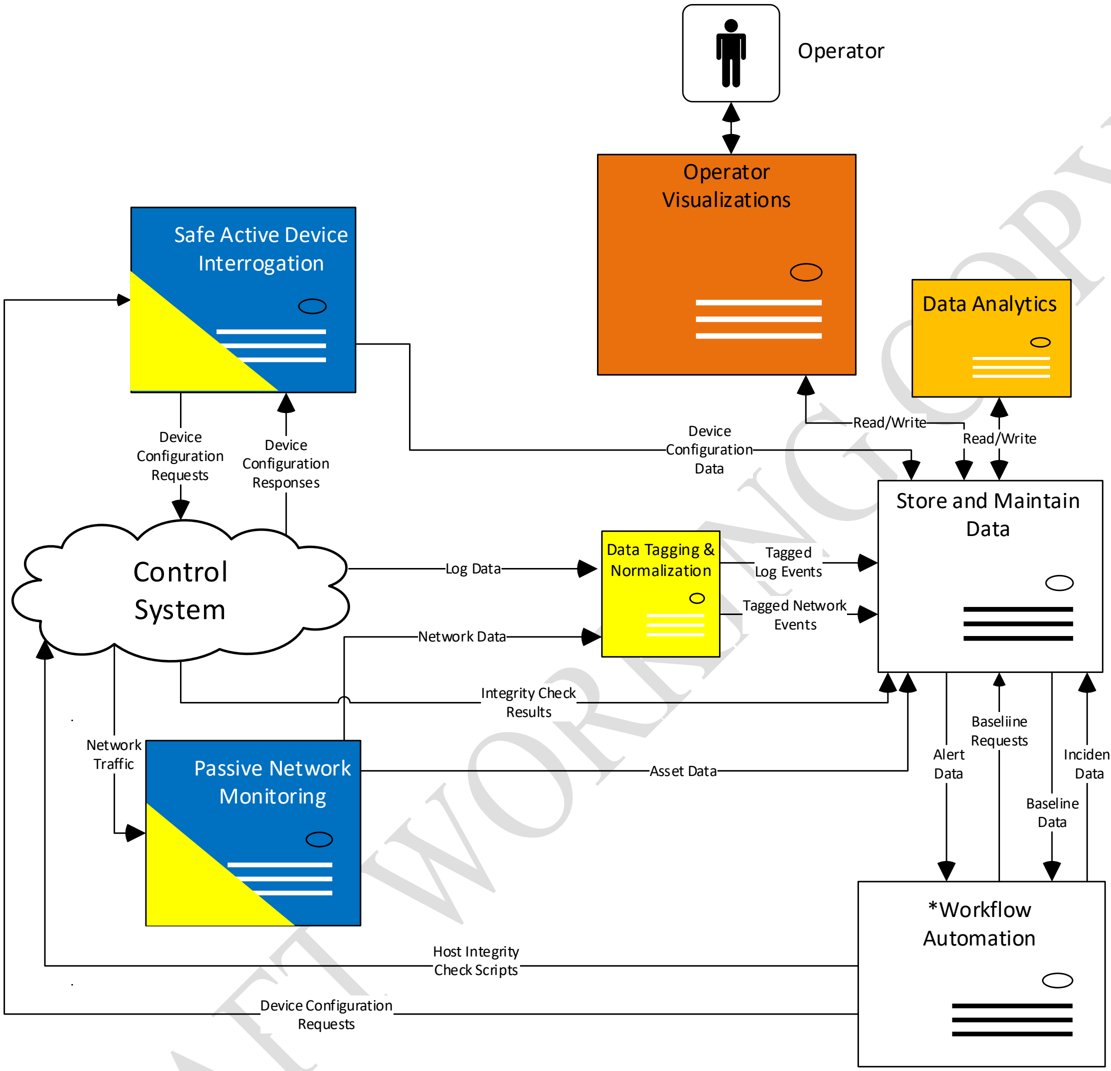
**Figure 3-6 MOSAICS Block 1 Visualization Functional Block Diagram**

## 3.2 MOSAICS Block 1 Reference Architecture



*Store and Maintain Data and Workflow Automation cross all Block 1 functions

Figure 3-7 shows a reference architecture for the key MOSAICS functions identified in Section 3.1 and the Block 1 data flows.



*Store and Maintain Data and Workflow Automation cross all Block 1 functions

**Figure 3-7 MOSAICS Block 1 Reference Architecture Data Flows**

# 4. BLOCK 1 FUNCTIONS AND REQUIREMENTS

Functional requirements are the highest level of MOSAICS system requirements, and the technical requirements are the next-level decomposition of the functional requirements. Functional and technical requirements for each MOSAICS function are provided in the following sections.

**NOTES:**

1. *The word "maintain," when used in the requirements, means to "create" and "update."*
2. *Devices within the "protected enclave" (see Section 6 Definitions) are monitored by MOSAICS. Some devices may not be actively monitored by MOSAICS (i.e., a remote site with limited connectivity, a device that speaks a different protocol, etc.).*

## 4.1 System Identification Requirements

The System Identification Functional Requirements and Technical Requirements are provided in Table 4-1 and Table 4-2, respectively.

**Table 4-1 System Identification Functional Requirements**

| ID | Requirement | Block |
|---|---|---|
| **F1.0** | **MOSAICS System Identification Requirements** | |
| **F1.1** | **Detect and Collect Asset Information** | |
| **F1.1.1** | MOSAICS shall detect assets on the network.<br>*Note: Assets include host, network equipment, and control equipment.* | 1A |
| **F1.2** | **Assign Asset Criticality** | |
| **F1.2.1** | MOSAICS shall provide the capability for the user to assign asset criticality.<br>*Note: Critical assets may be those that contribute to the facility's mission or are assessed as high-value.* | 1A |
| **F1.3** | **Maintain Inventory** | |
| **F1.3.1** | MOSAICS shall maintain an inventory of assets. | 1A |
| **F1.4** | **Create Baselines** | |
| **F1.4.1** | MOSAICS shall maintain a baseline of assets. | 1A |

**Table 4-2 System Identification Technical Requirements**

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **F1.0** | **MOSAICS System Identification Technical Requirements** | | |
| **F1.1** | **Detect and Collect Asset Information** | | |
| | *Passive Detection and Collection* | | |
| **T1.1.1.1** | MOSAICS shall be capable of automated, passive data collection via a local switch SPAN port or serial port. | F1.1.1 | 1A |
| **T1.1.1.2** | MOSAICS shall be capable of automated, passive data collection on control equipment that is not capable of Internet Protocol (IP) or not connected to the IP network.<br>*Note: This could include non-IP-addressable devices communicating through intermediary devices providing native communication protocol traffic encapsulated in IP.* | F1.1.1 | 1A |
| **T1.1.1.3** | MOSAICS shall be capable of automated, passive collection of the following control equipment information, at a minimum:<br>• IP address<br>• Media Access Control Address (MAC address)<br>• Vendor<br>• Protocols used | F1.1.1 | 1A |
| **T1.1.1.4** | MOSAICS shall be capable of automated, passive collection of the following host information, at a minimum, upon user demand:<br>• IP address<br>• MAC address<br>• Hostname<br>• OS type<br>• Protocols used | F1.1.1 | 1A |
| **T1.1.1.5** | MOSAICS shall be capable of automated, passive collection of the following network equipment information, at a minimum, upon user demand:<br>• IP address<br>• MAC address<br>• Hostname<br>• Protocols used | F1.1.1 | 1A |
| | *Manual Data collection*<br>*Note: In this manual collection case, the user collects the information and provides it to MOSAICS to ingest.* | | |
| **T1.1.1.6** | MOSAICS shall be capable of manually ingesting and processing control equipment information, upon user demand.<br>*Note: The manually ingestible control equipment information consists of the information that can be actively collected (see T1.1.1.11) and potentially additional information such as owner, location, etc.* | F1.1.1 | 1A |

| **Req Number** | **Requirement** | **Map to Funct Rqmts** | **Block** |
|---|---|---|---|
| **T1.1.1.7** | MOSAICS shall be capable of manually ingesting and processing host information, upon user demand:<br>*Note: The manually ingestible host information consists of the information that can be actively collected (see T1.1.1.12) and potentially additional information such as owner, location, etc.* | F1.1.1 | 1A |
| **T1.1.1.8** | MOSAICS shall be capable of manually ingesting and processing network equipment information, upon user demand:<br>*Note: The manually ingestible host information consists of the information that can be actively collected (see T1.1.1.13) and potentially additional information such as owner, location, etc.* | F1.1.1 | 1A |
| | *Safe Active Data Collection* | | |
| **T1.1.1.9** | MOSAICS shall be capable of automated, active data collection on control equipment that is not capable of IP or not connected to the IP network.<br>*Note: This could include non-IP-addressable devices communicating through intermediary devices providing native communication protocol traffic encapsulated in IP.* | F1.1.1 | 1A |
| **T1.1.1.10** | MOSAICS shall be capable of automated, active collection of the following control equipment information, at a minimum:<br>• IP address<br>• MAC address<br>• Vendor<br>• Protocols used<br>• Configuration data<br>• Ladder logic<br>• Logs<br>• Software/Firmware<br>• Hardware | F1.1.1 | 1A |
| **T1.1.1.11** | MOSAICS shall be capable of active collection of the following host information, at a minimum:<br>• IP address<br>• MAC address<br>• Hostname<br>• OS type<br>• OS version<br>• Vendor<br>• Registry entry values<br>• User accounts<br>• User profiles<br>• Processes<br>• Services<br>• Process network connections<br>• Installed drivers<br>• Log entries<br>• Peripheral devices | F1.1.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| | • HOST file hash<br>• LMHOST file hash<br>• Alternate Data Streams (ADSs)<br>• System Status<br>• Memory Status | | |
| **T1.1.1.12** | MOSAICS shall be capable active collection of the following network equipment information, at a minimum:<br>• IP address<br>• MAC address<br>• Hostname<br>• Vendor<br>• Interface files<br>• Network tables including routing tables<br>• ARP tables<br>• Dynamic Host Configuration Protocol (DHCP) server configuration files<br>• Access control lists<br>• Firewall or ipTables rules<br>• Users | F1.1.1 | 1A |
| **T1.1.1.12** | MOSAICS shall store the following in a common data repository.<br>• Inventory<br>• Baselines<br>*Note: This information is stored in a data repository for further investigative purposes.* | F1.1.1 | 1A |
| **F1.2** | **Assign Asset Criticality** | | |
| **T1.2.1.1** | MOSAICS shall provide the capability for the user to assign criticality to assets.<br>*Note: Critical assets may be those that contribute to the facility's mission or are assessed as high-value.* | F1.2.1 | 1A |
| **T1.2.1.2** | MOSAICS shall maintain asset criticality information.<br>*Note: This criticality information is used in T4.1.1.3 to determine alert severity and in Block 2 to prioritize responses based on threat and mission impact.* | F1.2.1 | 1A |
| **F1.3** | **Maintain Inventory**<br>*Note: Maintaining the inventory includes creating it and updating it.* | | |
| **T1.3.1.1** | MOSAICS shall maintain an inventory of control equipment.<br>*Note: Control equipment is identified by passive or active scanning and may also be identified manually (see T1.1.1.3 T1.1.1.10, and T1.1.1.6, respectively).* | F1.3.1 | 1A |
| **T1.3.1.2** | MOSAICS shall maintain an inventory of hosts.<br>*Note: Hosts are identified by passive or active scanning and may also be identified manually (see T1.1.1.4 T1.1.1.11, and T1.1.1.7, respectively).* | F1.3.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **T1.3.1.3** | MOSAICS shall maintain an inventory of network equipment.<br>*Note: Network equipment is identified by passive or active scanning and may also be identified manually (see T1.1.1.5 T1.1.1.12, and T1.1.1.8, respectively).* | F1.3.1 | 1A |
| **T1.3.1.4** | MOSAICS shall uniquely identify each asset in inventory.<br>*Note: The unique identification may be IP address, MAC address, or hostname, for example.* | F1.3.1 | 1A |
| **T1.3.1.5** | MOSAICS shall update asset inventories upon change in assets in the protected enclave.<br>*Note: This applies to all inventories (control equipment, hosts, and network equipment).* | F1.3.1 | 1A |
| **F1.4** | **Create Baselines**<br>*Note: When the system is first deployed, the user will create a baseline. An asset, or all assets, may be re-baselined upon user demand. These baselines are used by the Analysis function to identify deviations from the baselines.* | | |
| **T1.4.1.1** | MOSAICS shall create a baseline of user accounts and associated user profiles for hosts within the protected enclave, upon user demand. | F1.4.1 | 1A |
| **T1.4.1.2** | MOSAICS shall create a baseline of network communications between control equipment, hosts, and network equipment, upon user demand. | F1.4.1 | 1A |
| **T1.4.1.3** | MOSAICS shall create a baseline of control equipment, upon user demand. | F1.4.1 | 1A |
| **T1.4.1.4** | MOSAICS shall create a baseline of hosts, upon user demand. | F1.4.1 | 1A |
| **T1.4.1.5** | MOSAICS shall create a baseline of network equipment, upon user demand. | F1.4.1 | 1A |

Acronyms not defined within this table can be found in Appendix D.

## 4.2 System Protection Requirements

The System Protection Functional Requirements and Technical Requirements are provided in Table 4-3**Error! Reference source not found.** and Table 4-4, respectively.

**Table 4-3 System Protection Functional Requirements**

| ID | Requirement | Block |
|---|---|---|
| **F2.0** | **MOSAICS System Protection Requirements** | |
| **F2.1** | **Identity and Access Management Requirements** | |
| **F2.1.1** | MOSAICS shall manage access to MOSAICS, based on user identity and access permissions. | 1A |
| **F2.2** | **Data Security Requirements** | |

| ID | Requirement | Block |
|---|---|---|
| **F2.2.1** | MOSAICS shall protect the data collected by MOSAICS<br>*Note: Data stored must be encrypted.* | 1A |
| **F2.3** | **Audit Logging Requirements** | |
| **F2.3.1** | MOSAICS shall maintain audit logs for MOSAICS activities, in accordance with facility policies. | 1A |

**Table 4-4 System Protection Technical Requirements**

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **F2.0** | **MOSAICS System Protection Technical Requirements** | | |
| **F2.1** | **Identity and Access Management Technical Requirements** | | |
| **T2.1.1.1** | MOSAICS shall control access to MOSAICS using Role Based Access Control (RBAC).<br>*Note: The user and authorized device information is obtained for authoritative sources (see F2.1.4). This is not meant to imply that MOSAICS has an Active Directory of its own.* | F2.1.1 | 1A |
| **T2.1.1.2** | MOSAICS shall maintain the identities, credentials, and access permissions for authorized devices and users for MOSAICS.<br>*Note: This allows MOSAICS to integrate with facility Active Directory, for example.* | F2.1.1 | 1A |
| **T2.1.1.3** | MOSAICS shall access the identities and credentials for authorized devices and users maintained by Facility authoritative sources.<br>*Note: This is for local accounts maintained by MOSAICS.* | F2.1.1 | 1A |
| **F2.2** | **Data Security Technical Requirements** | | |
| **T2.2.1.1** | MOSAICS shall protect the data collected by MOSAICS while at rest.<br>*Note: Data stored must be encrypted.* | F2.2.1 | 1A |
| **T2.2.1.2** | MOSAICS shall protect the data in transit within the MOSAICS system, where feasible.<br>*Note: Data must be encrypted when sent between MOSAICS system components and between control equipment and MOSAICS, where feasible. "Where feasible" is used because some communications will not support encryption.* | F2.2.1 | 1A |
| **F2.3** | **Audit Logging Requirements** | | |
| **T2.3.1.1** | MOSAICS shall log the following activities, at a minimum:<br>• User access to MOSAICS components<br>• User-initiated actions<br>• All automated workflow executions<br>• Events and alerts<br>• Integrity check execution<br>• Actions performed (including provenance) | F2.3.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| | • Failed actions<br>• Errors<br>• State at time of a service interruption or system shutdown<br>*Note: Actions provenance includes associated information origin and decision rationale.* | | |
| **T2.3.1.2** | MOSAICS shall provide the ability to archive historical log data. | F2.3.1 | 1A |
| **T2.3.1.3** | MOSAICS shall provide the ability to recover previously archived historical log data. | F2.3.1 | 1A |

## 4.3 Monitor & Detection Requirements

The Monitor & Detection Functional Requirements and Technical Requirements are provided in Table 4-5 and Table 4-6, respectively.

**Table 4-5 Monitor & Detection Functional Requirements**

| ID | Requirement | Block |
|---|---|---|
| **F3.0** | **MOSAICS Monitor and Detection Requirements** | |
| **F3.1** | **Continuous Monitoring Requirements** | |
| **F3.1.1** | MOSAICS shall continuously monitor network communication within the protected enclave. | 1A |
| **F3.1.2** | MOSAICS shall continuously monitor the status of protected enclave assets. | 1A |
| **F3.2** | **Detection Requirements** | |
| **F3.2.1** | MOSAICS shall detect changes to the configuration of protected enclave assets. | 1A |
| **F3.2.2** | MOSAICS shall detect abnormal behavior of protected enclave assets. | 1A |
| **F3.2.3** | MOSAICS shall detect malicious indicators on protected enclave assets. | 1A |
| **F3.2.4** | MOSAICS shall detect changes to the configuration of protected enclave network communications. | 1A |
| **F3.2.5** | MOSAICS shall detect abnormal behavior of the protected enclave network communications. | 1A |
| **F3.2.6** | MOSAICS shall detect malicious indicators on the protected enclave network communications. | 1A |
| **F3.3** | **Event Generation** | |
| **F3.3.1** | MOSAICS shall generate an event whenever any detection criteria (e.g., change in behavior, access/usage rule violation) not captured in the baseline is triggered. | 1A |

**Table 4-6 Monitor & Detection Technical Requirements**

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **F3.0** | **MOSAICS Monitor and Detection Technical Requirements** | | |
| **F3.1** | **Continuous Monitoring Technical Requirements** | | |
| **T3.1.1** | MOSAICS shall collect communication data on the protected enclave network (e.g., full-packet captures for IP-based networks) | F3.1.1 | 1A |
| **T3.1.2** | MOSAICS shall collect the following data for protected enclave control equipment assets, including at a minimum:<br>• IP address<br>• MAC address<br>• Vendor<br>• Protocols used | F3.1.2 | 1A |
| **T3.1.2** | MOSAICS shall collect the following data for protected enclave network equipment assets, including at a minimum:<br>• IP address<br>• MAC address<br>• Hostname<br>• Protocols used | F3.1.2 | 1A |
| **T3.1.2** | MOSAICS shall collect the following data for protected enclave hosts, as a minimum:<br>• IP address<br>• MAC address<br>• Hostname<br>• OS type | F3.1.2 | 1A |
| **F3.2** | **Detection Requirements** | | |
| **T3.2.1** | MOSAICS shall detect changes to the configuration of protected enclave control equipment assets, including at a minimum:<br>• Reconfiguration: Firmware, Logic, settings, etc.<br>• Connections: New or external networks | F3.2.1 | 1A |
| **T3.2.2** | MOSAICS shall detect changes in the behavior on protected enclave control equipment assets, including at a minimum:<br>• Account actions: Add or remove privileges, unsuccessful login, etc.<br>• Remote Access: SSH, FTP, etc. | F3.2.2 | 1A |
| **T3.2.3** | MOSAICS shall detect changes to the configuration of protected enclave network equipment assets, including at a minimum:<br>• Reconfiguration: Firmware, Logic, settings, etc.<br>• Connections: New or external networks | F3.2.1 | 1A |
| **T3.2.4** | MOSAICS shall detect changes in the behavior of protected enclave network equipment assets, including at a minimum:<br>• Account actions: Add or remove, privileges, unsuccessful login, etc.<br>• Remote Access: SSH, FTP, etc. | F3.2.2 | 1A |
| **T3.2.4** | MOSAICS shall detect changes to the configuration of protected enclave host assets, including at a minimum: | F3.2.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| | • User accounts<br>• User profiles<br>• Processes<br>• Services<br>• Process network connections<br>• Installed drivers<br>• Log entries<br>• Peripheral devices<br>• Memory status<br>• Executable file creation | | |
| **T3.2.5** | MOSAICS shall detect changes of process and service behavior of protected enclave hosts, including at a minimum:<br>• Installation: Applications, services, tasks, etc.<br>• Remote Access: RDP, WMI, etc.<br>• Shell: Command prompt, PowerShell, etc.<br>• Connections: Process reach out, external networks, shares | F3.2.2 | 1A |
| **T3.2.6** | MOSAICS shall detect changes of peripheral device behavior of protected enclave hosts, including at a minimum:<br>• Peripherals: USBs, removable devices, etc. | F3.2.2 | 1A |
| **T3.2.7** | MOSAICS shall detect changes in user/account behavior of protected enclave hosts, including at a minimum:<br>• Account actions: Add or remove, privileges, unsuccessful login, etc. | F3.2.2 | 1A |
| **T3.2.8** | MOSAICS shall detect changes in file behavior of protected enclave hosts.<br>*Note: An executable file could start acting in an unexpected manner (unexpected memory access, for example).* | F3.2.2 | 1A |
| **T3.2.9** | MOSAICS shall detect a malicious file signature on a protected enclave asset. | F3.2.3 | 1A |
| **T3.2.10** | MOSAICS shall detect changes in protected enclave network traffic communication configuration, including at a minimum:<br>• Changes in protocols present<br>• Changes in IP addresses | F3.2.4 | 1A |
| **T3.2.11** | MOSAICS shall detect anomalous protected enclave network traffic behavior, including at a minimum:<br>• Changes in volume of network traffic<br>• Changes in timing of network traffic | F3.2.5 | 1A |
| **T3.2.12** | MOSAICS shall detect when a malicious network traffic signature is present on the protected enclave network. | F3.2.6 | 1A |
| **F3.3** | **Event Generation** | | |
| **T3.3.1** | MOSAICS shall store events in a common data repository.<br>*Note: This information is stored in a data repository for further investigative purposes.* | F3.3.1 | 1A |
| **T3.3.2** | MOSAICS shall generate an event within 1 minute of the activity resulting in the event. | F3.3.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **T3.3.3** | MOSAICS shall categorize events with a normalized event tag.<br>*Note: The tag is for use in analysis.* | F3.3.1 | 1A |
| **T3.3.4** | MOSAICS events shall include the following, at a minimum:<br>• All accompanying data elements used to generate the event<br>• Timestamp of when event created<br>• Normalized event tag<br>• Unique identifier | F3.3.1 | 1A |

Acronyms not defined within this table can be found in Appendix D.

## 4.4 Analysis Requirements

The Analysis Functional Requirements and Technical Requirements are provided in Table 4-7 and Table 4-8, respectively.

**Table 4-7 Analysis Functional Requirements**

| ID | Requirement | Block |
|---|---|---|
| **F4.0** | **MOSAICS Analysis Requirements** | |
| **F4.1** | **Analyze Events** | |
| **F4.1.1** | MOSAICS shall analyze events.<br>*Note: Event analysis includes correlating events, generating alerts, and assigning severity levels.* | 1A |
| **F4.2** | **Perform Integrity Checks** | |
| **F4.2.1** | MOSAICS shall perform integrity checks.<br>*Note: Integrity checks are performed when alerts are generated.* | 1B |

**Table 4-8 Analysis Technical Requirements**

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **F4.0** | **MOSAICS Analysis Technical Requirements** | | |
| **F4.1** | **Analyze Events** | | |
| **T4.1.1.1** | MOSAICS shall correlate events across assets, network communications, and time for analysis.<br>*Note: Events are correlated across sensors based on relationships identified between events within a specific block of time. Time for analysis is 5 minutes, per T4.1.1.8.* | F4.1.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **T4.1.1.2** | MOSAICS shall generate an alert based on predefined threat patterns of behavior.<br>*Note: Alerts may be based on a single event or multiple correlated events. Alerts are sent to the Visualization function for display to the user.* | F4.1.1 | 1A |
| **T4.1.1.3** | MOSAICS shall determine severity levels for alerts based on the following, at a minimum:<br>• Number of correlated events<br>• Integrity check results<br>• Criticality of the asset<br>*Note: See T1.2.1.2 for asset criticality assignment. See T4.2.1.1 for integrity checks.* | F4.1.1 | 1A |
| **T4.1.1.4** | MOSAICS shall include the following information relevant to the alert, at a minimum, when generating an alert:<br>• The event(s) resulting in the alert<br>• The associated assets<br>• Alert severity<br>• Integrity check results | F4.1.1 | 1A |
| **T4.1.1.5** | MOSAICS shall provide the user the capability to identify an alert as an incident.<br>*Note: Alerts may be identified as an incident by a user or by MOSAICS through Artificial Intelligence/Machine Learning (AI/ML) (see T4.1.1.6).* | F4.1.1 | 1A |
| **T4.1.1.6** | MOSAICS shall identify an alert as an incident.<br>*Note: Alerts may be identified as an incident by a user or by MOSAICS through AI/ML. (see T4.1.1.5).* | F4.1.1 | 1A |
| **T4.1.1.7** | MOSAICS shall store the following in a common data repository.<br>• Alerts and associated information (includes integrity check results)<br>• Incidents and associated information<br>*Note: This information is stored in a data repository for further investigative purposes.* | F4.1.1 | 1A |
| **T4.1.1.8** | MOSAICS shall generate alerts within 5 minutes of generation of events.<br>*Note: This requirement drives the block of time used in T4.1.1.1.* | F4.1.1 | 1A |
| **F4.2** | **Perform Integrity Checks**<br>*Note: The integrity check is performed through automation by comparing observed values with baseline normal values.* | | |
| **T.4.2.1.1** | MOSAICS shall automatically identify required integrity checks to perform based on alert type.<br>*Note: Integrity checks are those related to that specific alert type, and may include data for control equipment, host, or* | F4.2.1 | 1B |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| | *network equipment, as well as user accounts and network communications.* | | |
| **T4.2.1.2** | MOSAICS shall automatically collect the following control equipment information, at a minimum, when performing an integrity check:<br>• IP address<br>• MAC address<br>• Vendor<br>• Protocols used<br>• Configuration data<br>• Ladder logic<br>• Logs<br>• Software/Firmware<br>• Hardware<br>*Note: This is the full set of data that can be collected through active collection (see T1.1.1.10). A subset is collectable through passive collection (T1.1.1.3).* | F4.2.1 | 1B |
| **T4.2.1.3** | MOSAICS shall automatically collect the following host information, at a minimum, when performing an integrity check:<br>• IP address<br>• MAC address<br>• Hostname<br>• OS type<br>• OS version<br>• Vendor<br>• Registry entry values<br>• User accounts<br>• User profiles<br>• Processes<br>• Services<br>• Process network connections<br>• Installed drivers<br>• Log entries<br>• Peripheral devices<br>• HOST file hash<br>• LMHOST file hash<br>• ADS<br>• System Status<br>• Memory Status<br>*Note: This is the full set of data that can be collected through active collection (see T1.1.1.11). A subset is collectable through passive collection (T1.1.1.4).* | F4.2.1 | 1B |
| **T4.2.1.4** | MOSAICS shall automatically collect the following network equipment information, at a minimum, when performing an integrity check:<br>• IP address | F4.2.1 | 1B |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
|  | • MAC address<br>• Hostname<br>• Vendor<br>• Interface files<br>• Network tables including routing tables<br>• ARP tables<br>• DHCP server configuration files<br>• Access control lists<br>• Firewall or ipTables rules<br>• Users<br>*Note: This is the full set of data that can be collected through active collection (see T1.1.1.12). A subset is collectable through passive collection (T1.1.1.5).* |  |  |
| **T4.2.1.5** | MOSAICS shall automatically compare data collected for integrity checks with the baseline for the data.<br>*Note: See T.4.2.1.1 through T.4.2.1.3 for data collected. See T1.4.1.1 through T1.4.1.5 for baselines.* | F4.2.1 | 1B |
| **T4.2.1.6** | MOSAICS shall automatically generate integrity check results that include the following, at a minimum:<br>• Differences between data collected for integrity check and the baseline<br>• Errors encountered when performing the integrity check<br>*Note: Integrity check results are used when determining alert severity (see T4.1.1.3) and are provided with generated alerts (see T4.1.1.4).* | F4.2.1 | 1B |
| **T4.2.1.6** | MOSAICS shall complete integrity checks within 15 minutes of alert generation. | F4.2.1 | 1B |

## 4.5 Visualization

The Visualization Functional Requirements and Technical Requirements are provided in Table 4-9 and Table 4-10, respectively.

**Table 4-9 Visualization Functional Requirements**

| ID | Requirement | Block |
|---|---|---|
| **F5.0** | **MOSAICS Visualization Requirements** |  |
| **F5.1** | **Detected Event Visualization Requirements** |  |
| **F5.1.1** | MOSAICS shall provide the capability to visualize detected events. | 1A |
| **F5.2** | **Protected Enclave Status Visualization Requirements** |  |
| **F5.2.1** | MOSAICS shall provide the capability to visualize the protected enclave status. | 1A |

| ID | Requirement | Block |
|---|---|---|
| **F5.3** | **Alert Visualization and Management Requirements** | |
| **F5.3.1** | MOSAICS shall provide the capability to manage alerts. | 1B |
| **F5.3.2** | MOSAICS shall provide the capability to visualize alerts. | 1A |
| **F5.4** | **Orchestration and Metric Visualization Requirements** | |
| **F5.4.1** | MOSAICS shall provide the capability to visualize performance metrics related to Orchestration. | 1B |

**Table 4-10 Visualization Technical Requirements**

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **F5.0** | **MOSAICS Visualization Technical Requirements** | | |
| **F5.1** | **Detected Event Visualization Technical Requirements** | | |
| **T5.1.1.1** | MOSAICS shall allow a user to perform searches on event data. | F5.1.1 | 1A |
| **T5.1.1.2** | MOSAICS shall allow a user to perform sorts on event data. | F5.1.1 | 1A |
| **T5.1.1.3** | MOSAICS shall allow a user to perform filtering on event data. | F5.1.1 | 1A |
| **T5.1.1.4** | MOSAICS shall perform trending and charting of event data. | F5.1.1 | 1A |
| **F5.2** | **Protected Enclave Status Visualization Technical Requirements** | | |
| **T5.2.1.1** | MOSAICS shall allow the user to view logs, events, and alerts. | F5.2.1 | 1A |
| **T5.2.1.2** | MOSAICS shall provide the capability to display which asset of the protected enclave has been affected by alerts and events. | F5.2.1 | 1A |
| **T5.2.1.3** | MOSAICS shall provide the capability to display device identifying properties of devices monitored by MOSAICS. At a minimum this will include:<br>• IP address<br>• MAC address<br>• Device model<br>• Device serial number<br>• Property owners<br>• Internal property number | F5.2.1 | 1A |
| **T5.2.1.4** | MOSAICS shall provide the capability to display the user accounts logged into assets monitored by MOSAICS.<br>*Note: This includes both network and host assets.* | F5.2.1 | 1A |
| **T5.2.1.5** | MOSAICS shall provide the capability to display the current communication protocols used by an asset monitored by MOSAICS. | F5.2.1 | 1A |
| **T5.2.1.6** | MOSAICS shall display a page that is dedicated to displaying the health and status of specific assets.<br>*Note: This includes problematic credentials on network and host assets.* | F5.2.1 | 1A |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **T5.2.1.7** | MOSAICS shall provide the capability to visualize baseline information for each asset.<br>*Note: The assets include control equipment, hosts, and network equipment.* | F5.2.1 | 1A |
| **T5.2.1.8** | MOSAICS shall provide the capability to visualize a current map of network communication flows between control equipment, hosts, and network devices.<br>*Note: This map is generated from live network communication.* | F5.2.1 | 1A |
| **F5.3** | **Alert Visualization and Management Technical Requirements** | | |
| **T5.3.1.1** | MOSAICS shall provide the capability for the user to acknowledge displayed alerts. | F5.3.1 | 1B |
| **T5.3.1.2** | MOSAICS shall provide the capability to assign alerts. | F5.3.1 | 1B |
| **T5.3.1.3** | MOSAICS shall provide the capability to open/close alerts. | F5.3.1 | 1B |
| **T5.3.2.1** | MOSAICS shall have the capability to visualize any alert. | F5.3.2 | 1A |
| **T5.3.2.2** | MOSAICS shall have the capability to see correlated events for a given alert. | F5.3.2 | 1A |
| **T5.3.2.3** | MOSAICS shall have the capability to visualize incidents. | F5.3.2 | 1A |
| **T5.3.2.4** | MOSAICS shall provide the ability to search, sort, and filter alerts by data attributes, which at a minimum will include:<br>• IP addresses<br>• MAC addresses<br>• Device serial numbers<br>• Property owners<br>• Device models<br>• Logins<br>• Process IDs<br>• Priority<br>• Date/time<br>• Severity | F5.3.2 | 1A |
| **T5.3.2.5** | MOSAICS shall provide the ability to display all integrity checks triggered by an alert. | F5.3.2 | 1B |
| **T5.3.2.6** | MOSAICS shall display the results of integrity checks triggered by an alert within 5 seconds of completion of the integrity check.<br>*Note: The results of the integrity checks include errors encountered by the integrity checks if they failed for any reason.* | F5.3.2 | 1B |
| **T5.3.2.7** | MOSAICS shall perform trending and charting of alert/incident data. | F5.3.2 | 1A |
| **F5.4** | **Orchestration and Metric Visualization Requirements** | | |
| **T5.4.2.1** | MOSAICS shall provide visualizations capable of displaying metrics regarding the state of the orchestrator. | F5.4.2 | 1B |
| **T5.4.2.2** | MOSAICS shall provide visualizations capable of displaying metrics regarding playbook time to completion. | F5.4.2 | 1B |

| Req Number | Requirement | Map to Funct Rqmts | Block |
|---|---|---|---|
| **T5.4.2.3** | MOSAICS shall display an alert within 5 seconds of alert generation. | F5.4.2 | 1A |

Acronyms not defined within this table can be found in Appendix D.

# 5. DEPLOYMENT CONSIDERATIONS

The following should be considered when deploying MOSAICS:

1. **Shared Goals and Objectives:** It is important to socialize ideas across the organization in order to drive interest, support, and commitment. Ensuring a shared understanding of the threat, the need for improved operational technology (OT) cybersecurity, and the goals and objectives with the implementation of MOSAICS is essential to acceptance of these capabilities.

2. **Build Trust:** Building trust in the use of MOSAICS and that it does not pose a risk to operations is essential. Implementing the passive monitoring capabilities defined in MOSAICS Block 1A, expanding into safe active monitoring of Block 1B, and maturing the capabilities with Block 2 concepts are great ways to demonstrate value and build trust over time.

3. **Product Integration:** When selecting capabilities for the control system environment, consider implications for the ability to automate data collection and investigation processes. The right functionality must be exposed through Application Programming Interfaces (API) in order to gain efficiencies via automation and to leverage new capabilities in operations.

4. **Sustainment:** Consider long-term sustainment of the MOSAICS capabilities up front. As new sensors or data sources are added to the environment, organizations must ensure they have the skills required to integrate new products, incorporate new alerts, and build visualization dashboards for improved operational efficiency.

5. **Asset Discovery and Enumeration:** Limitations exist in the amount of detailed data that can be obtained through the passive discovery means defined in Block 1A. Safe active enumeration techniques (Block 1B) provide the capability to monitor and alert on changes to the environment at a much more granular level and are considered essential to full Block 1 implementation.

6. **OT Technology Enumeration:** Matching a discovery and enumeration capability to the control system for which it will be used is vital to ensuring the most effective solution. Some products are found to be simply better at identifying and enumerating specific control system technologies than others. This is especially true when utilizing active enumeration techniques because the interfaces need to be designed for specific vendor technologies. However, this can also be seen when simply parsing passive network traffic, and thus it is critical to understand what control system technologies are supported by a vendor prior to acquisition.

7. **Data Ingestion:** The ability to consume and correlate data from sensors deployed across all layers of an ICS architecture is vital for robust threat detection. Interfaces specifically for ICS sensors and data are lacking in comparison to IT tools, therefore the ability to develop custom plug-ins or connectors ensures that relevant data can be made available for analysis.

8. **Alerting and Correlation:** Adversaries often adapt their tactics and techniques to the environment they are attacking. While some threat activity will always occur prior to other events, it is essential that a threat be detected, regardless of the sequential order in which these events occur. The ability to support non-sequential event correlation for detection and alerting is a critical component for the selected analytic platform. This ensures that a minor change in adversary tactics will not result in missing threat activity.

9. **Operational Availability:** MOSAICS operational availability will be determined by the facility owner. MOSAICS must not degrade the operational availability of the control equipment, network equipment, or hosts (i.e., Do no harm) and not adversely impact other connected systems (e.g., Control System Platform Enclave).

# 6. DEFINITIONS

| Term | Definition |
|---|---|
| Alerts | Notifications of event(s) that need operator attention. Alerts may be based on a single event or multiple correlated events. |
| Asset | Physical or logical object owned or under custodial duties of an organization (ISA-62443) All assets referred to are either host, network equipment, or control equipment. |
| Control Equipment | Asset: Class that includes distributed control systems (DCSs), programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, associated operators interface consoles, and field sensing and control devices used to manage and control the process (ISA-62443) |
| Protected Enclave | A set of system resources that operate in the same security domain and share the protection of a single, common, continuous security perimeter, monitored and protected by the MOSAICS System. |
| Events | An event is a captured change in the environment, including low-level occurrences (MS Windows log events, Intrusion Detection System (IDS) events, for example). |
| Host | Asset: Physical or logical computer that is attached to a communication subnetwork or inter-network and can use services provided by the network to exchange data with another attached system (ISA-62443). |
| Incident | An alert that requires an action. Operators may make the determination that an alert is an incident. An AI/ML function could also potentially make this determination in MOSAICS. |
| Industrial Control System (ICS) | A general term that encompasses several types of control systems, including SCADA systems, DCSs, and other control system configurations such as PLCs, often found in industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). |
| Integrity Check | Identifies deviations from the baseline. |
| MOSAICS Capability | Implemented instantiation of the MOSAICS framework. A collection of integrated technologies which satisfy, at a minimum, MOSAICS Block 1A. |
| MOSAICS Framework | A framework defining a body of functions and requirements for control system cyber threat defense organized into blocks. |
| Network Communication | The process of exchanging information between two or more devices connected to a network. This includes IP- and non-IP-based communications. |
| Network Equipment | Asset*:* Class that includes switches, routers, firewalls, gateways, and media converters used to manage and control the network communications. |
| Network Traffic | Computer network communications that are carried over wired or wireless networks between hosts. |
| Safe Active Enumeration | Uses the native protocols of the device so as not to negatively impact the device. |

# 7. REFERENCES

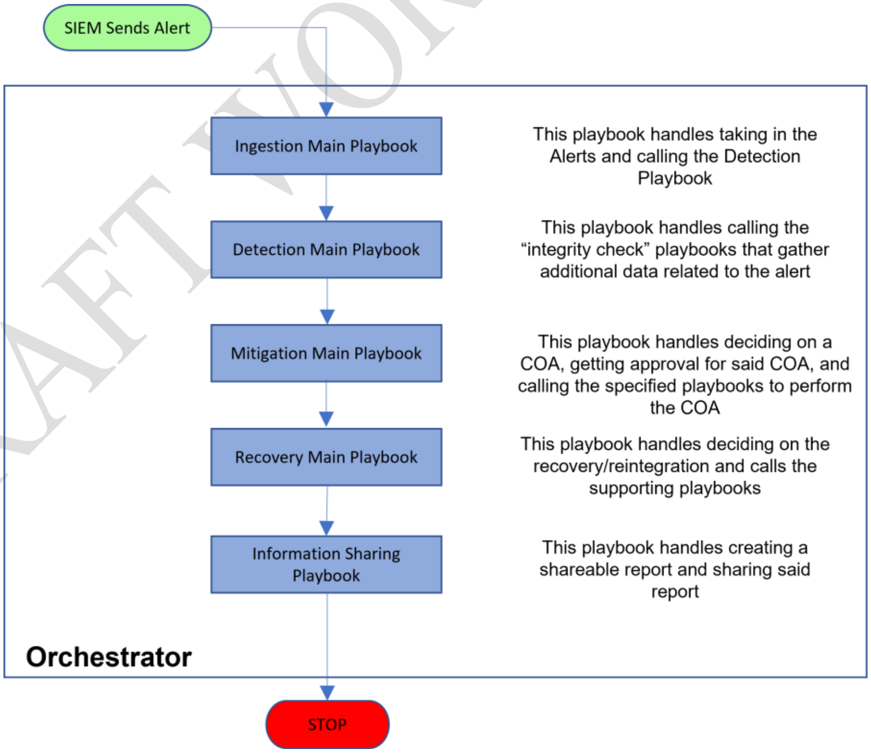
1. Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS), Revision 2, March 2018
2. More Situational Awareness for ICS (MOSAICS) Analysis of Alternatives, Johns Hopkins University Applied Physics Laboratory, AOS-23-0207, 14 February 2023
3. MOSAICS Final Report, Johns Hopkins University Applied Physics Laboratory, AOS-20-1416, October 2020

# APPENDIX A. AUTOMATION HIERARCHY AND WORKFLOW EXAMPLES

## A.1 MOSAICS Workflow Hierarchy

MOSAICS leverages SOAR automation capabilities to perform a number of critical functions within the system. Automation is first used to model and baseline the ICS network, capturing the appropriate configuration and operational state of each component. The core MOSAICS components utilize this knowledge, along with available data from various sensors, logs, and auditing components, to recognize defined sets of behaviors that are indicative of potential threat activity. The SOAR capability then leverages integrations that make on-demand requests of these devices for additional enrichment information, as appropriate, based on the category of the alert. The alerts and corresponding data are made available to the ICS operators who can choose to address the related incidents with response actions. Once the appropriate actions are determined, the SOAR platform executes response actions chosen by the operator in an automated fashion, enabling more effective scale and speed in identifying and mitigating incidents within the ICS system.

The MOSAICS automation design implements a main, top-level SOAR workflow for each of the core functions of alert ingestion, detection, mitigation, recovery, and information sharing, as shown in Figure A-1. These main workflows have supporting sub-workflows that can be called to implement specific functionality.


SIEM Sends Alert
Ingestion Main Playbook
This playbook handles taking in the Alerts and calling the Detection Playbook
Detection Main Playbook
This playbook handles calling the "integrity check" playbooks that gather additional data related to the alert
Mitigation Main Playbook
This playbook handles deciding on a COA, getting approval for said COA, and calling the specified playbooks to perform the COA
Recovery Main Playbook
This playbook handles deciding on the recovery/reintegration and calls the supporting playbooks
Information Sharing Playbook
This playbook handles creating a shareable report and sharing said report
Orchestrator
STOP

SIEM: Security Information and Event Management; COA: Course of Action

**Figure A-1 MOSAICS Hierarchy Design**

Figure A-2 shows the next level of detail of the workflow design. This demonstrates how workflows are broken down to call supporting sub-workflows, which allows for easy extensibility as new alerts, mitigation, and response actions are added to the system.

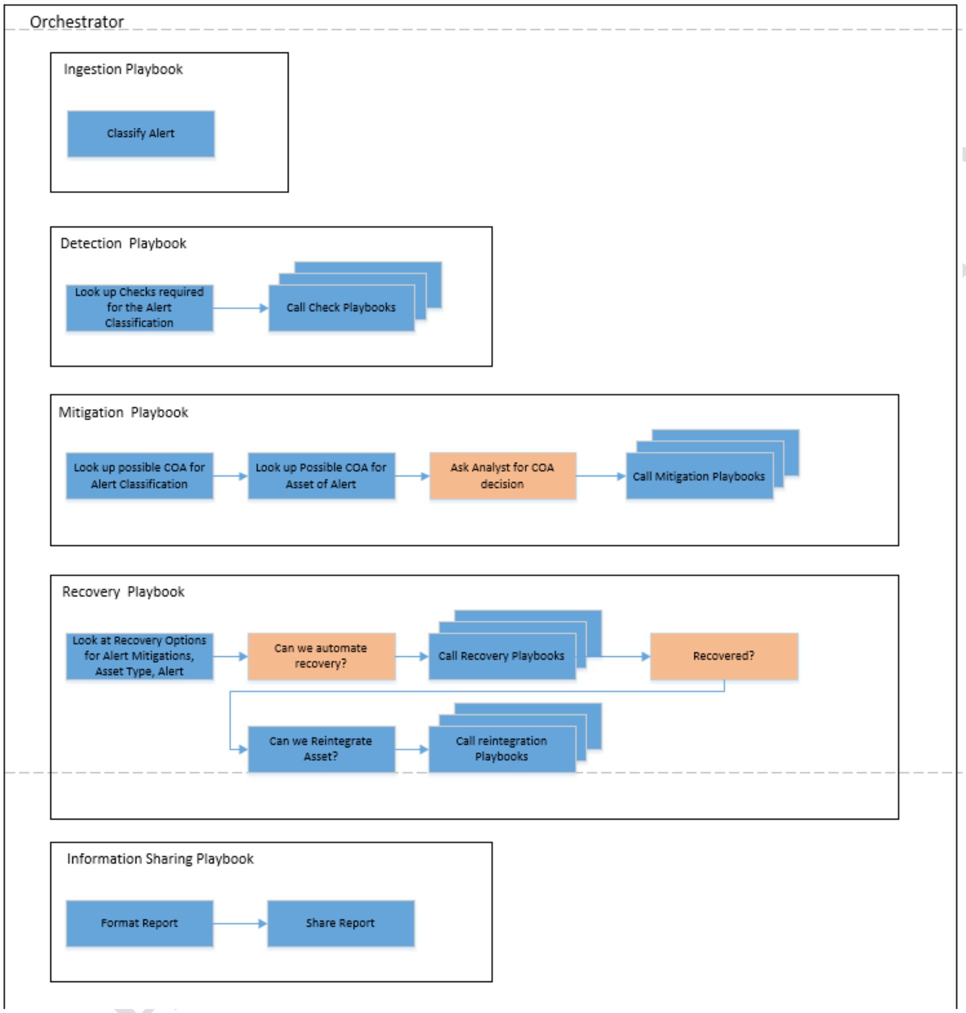

Orchestrator
Ingestion Playbook
Classify Alert
Detection Playbook
Look up Checks required for the Alert Classification
Call Check Playbooks
Mitigation Playbook
Look up possible COA for Alert Classification
Look up Possible COA for Asset of Alert
Ask Analyst for COA decision
Call Mitigation Playbooks
Recovery Playbook
Look at Recovery Options for Alert Mitigations, Asset Type, Alert
Can we automate recovery?
Call Recovery Playbooks
Recovered?
Can we Reintegrate Asset?
Call reintegration Playbooks
Information Sharing Playbook
Format Report
Share Report

**Figure A-2 MOSAICS Detailed View of Workflow Architecture**

## A.2 MOSAICS Workflow Execution

> ***Note:*** *While not all workflows described here are required for a MOSAICS Block 1 implementation, the full design is presented due to the interdependencies of the workflows and to ensure clarity of the automated processes.*

This section will utilize workflows developed for the MOSAICS Joint Capability Technology Demonstration (JCTD)[2], represented using Business Process Modeling Notation, to illustrate the execution of the MOSAICS workflow hierarchy. These workflows are used simply as examples of how the automation in MOSAICS can be implemented, but are not intended to be prescriptive.

[2] MOSAICS Final Report

Workflows built for a MOSAICS implementation will need to be adjusted to accommodate differing control system environments and/or orchestration platforms.

### A.2.1 Alert Processing Workflow Execution

The Main_Ingestion workflow (Figure A-3) is triggered by the SIEM flagging an event or series of events as suspicious and creating an alert. The alert tag designation is checked to determine what, if any, additional integrity checks are required to be executed against the associated control system assets. If no additional action is necessary, the alert is logged and workflow execution ends. However, if additional checks are required, the assets are placed in a maintenance mode and execution is passed to the detection workflow.

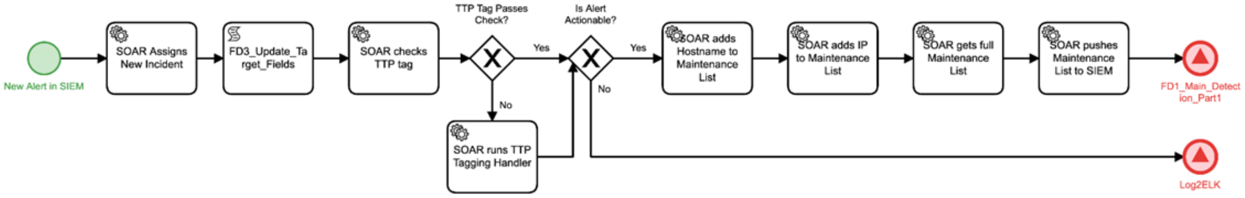
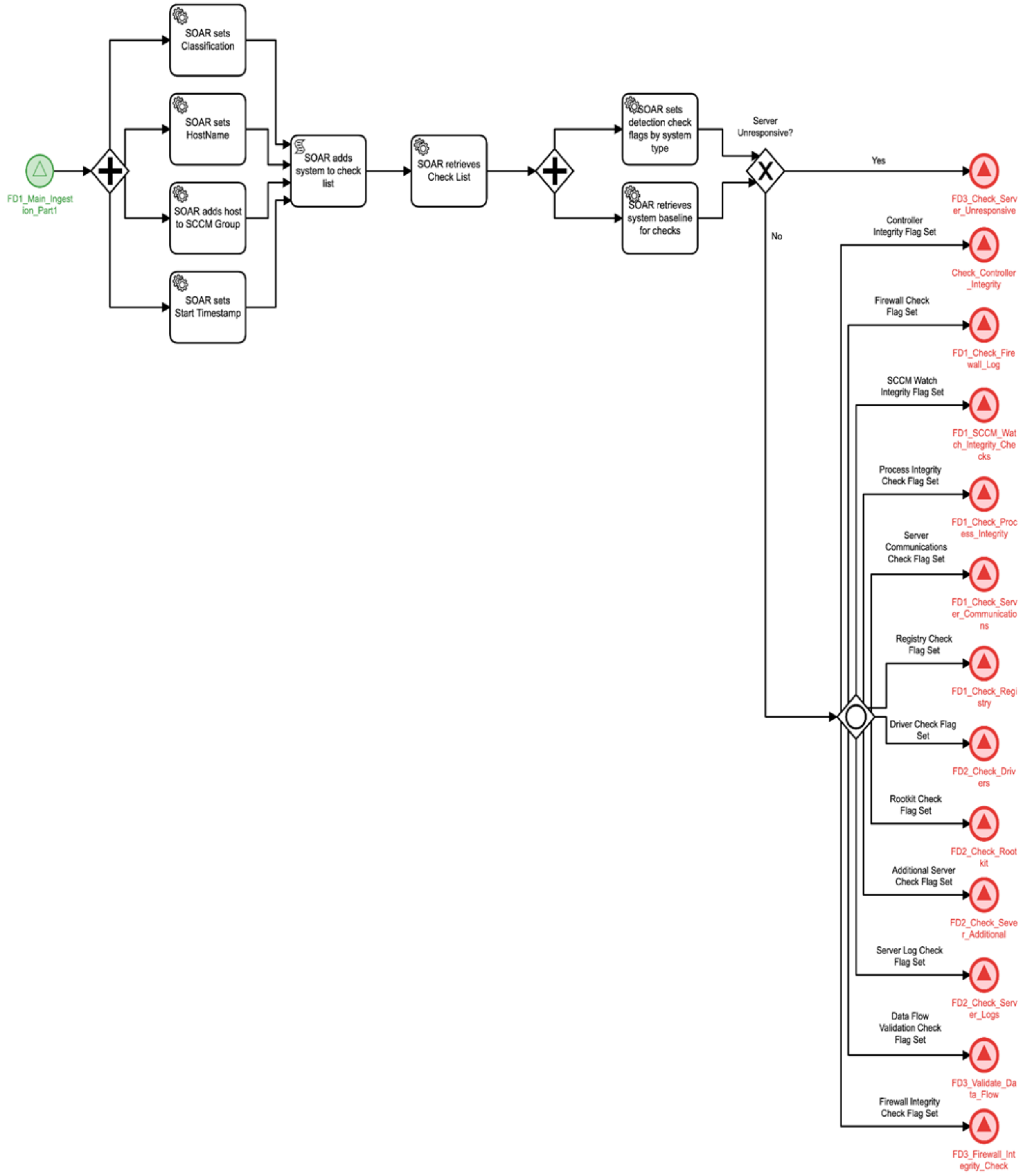

New Alert in SIEM
SOAR Assigns New Incident
FD3_Update_Target_Fields
SOAR checks TTP tag
TTP Tag Passes Check?
Yes
No
SOAR runs TTP Tagging Handler
Is Alert Actionable?
Yes
No
SOAR adds Hostname to Maintenance List
SOAR adds IP to Maintenance List
SOAR gets full Maintenance List
SOAR pushes Maintenance List to SIEM
FD1_Main_Detection_Part1
Log2ELK

**Figure A-3 FD1_Main_Ingestion_Part1**

The Main_Detection workflow (Figure A-4) examines the classification of the alert and then obtains the list of associated Integrity Checks for that alert and asset type (e.g., Windows host, firewall, controller). Prior to executing any Integrity Checks, the workflow ensures that the asset is reachable and obtains all baseline information for the associated asset that will be used by the Integrity Checks. The detection workflow then executes the list of identified Integrity Checks in sequence to determine whether any additional anomalies or suspicious events exist.


FD1_Main_Ingest ion_Part1
SOAR sets Classification
SOAR sets HostName
SOAR adds host to SCCM Group
SOAR sets Start Timestamp
SOAR adds system to check list
SOAR retrieves Check List
SOAR sets detection check flags by system type
SOAR retrieves system baseline for checks
Server Unresponsive?
Yes
No
FD3_Check_Serv er_Unresponsive
Controller Integrity Flag Set
Check_Controller _Integrity
Firewall Check Flag Set
FD1_Check_Fire wall_Log
SCCM Watch Integrity Flag Set
FD1_SCCM_Wat ch_Integrity_Che cks
Process Integrity Check Flag Set
FD1_Check_Proc ess_Integrity
Server Communications Check Flag Set
FD1_Check_Serv er_Communicatio ns
Registry Check Flag Set
FD1_Check_Regi stry
Driver Check Flag Set
FD2_Check_Driv ers
Rootkit Check Flag Set
FD2_Check_Root kit
Additional Server Check Flag Set
FD2_Check_Seve r_Additional
Server Log Check Flag Set
FD2_Check_Serv er_Logs
Data Flow Validation Check Flag Set
FD3_Validate_Da ta_Flow
Firewall Integrity Check Flag Set
FD3_Firewall_Int egrity_Check

SCCM: System Center Configuration Manager

**Figure A-4 FD1_Main_Detection_Part1**

Two representative samples of the Integrity Check workflows are shown in Figure A-5 and Figure A-6. In each case, the SOAR collects the most recent data from the asset, in these examples running processes and specific registry values, and compares that data to the baseline data collected previously. Results of this comparison are captured and execution is returned to the Main_Detection workflow.

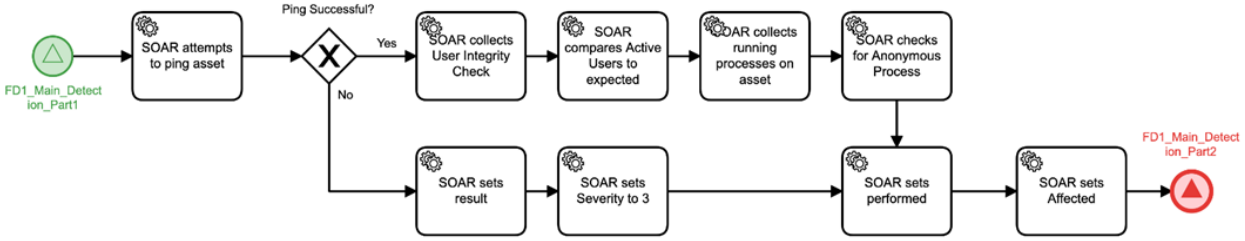

FD1_Main_Detection_Part1
SOAR attempts to ping asset
Ping Successful?
Yes
No
SOAR collects User Integrity Check
SOAR compares Active Users to expected
SOAR collects running processes on asset
SOAR checks for Anonymous Process
SOAR sets result
SOAR sets Severity to 3
SOAR sets performed
SOAR sets Affected
FD1_Main_Detection_Part2

**Figure A-5 FD1_Check_Process_Integrity**

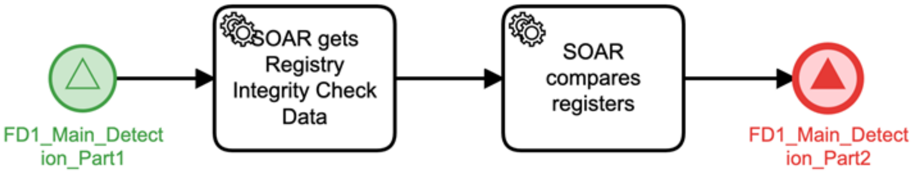
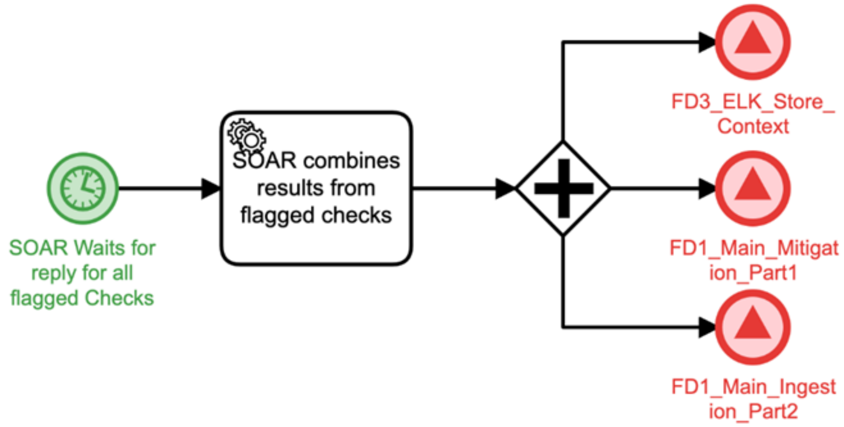


**Figure A-6 FD1_Check_Registry**

The Main_Detection workflow (Figure A-7) waits for completion of all Integrity Checks, and the results are logged back to the SIEM platform where it can be associated with the original alert. At this point, execution is passed back to the Main_Ingestion workflow, where the assets are removed from the maintenance list and the alert investigation is closed (Figure A-8).


SOAR Waits for reply for all flagged Checks
SOAR combines results from flagged checks
FD3_ELK_Store_Context
FD1_Main_Mitigation_Part1
FD1_Main_Ingestion_Part2

ELK: Elastic Search, Logstash, and Kibana

**Figure A-7 FD1_Main_Detection_Part2**

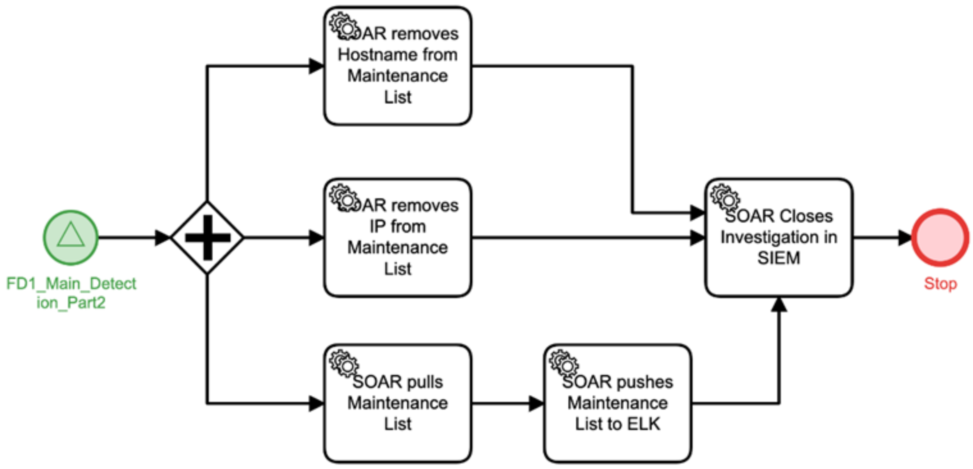

SOAR removes Hostname from Maintenance List
SOAR removes IP from Maintenance List
SOAR pulls Maintenance List
SOAR pushes Maintenance List to ELK
SOAR Closes Investigation in SIEM
FD1_Main_Detection_Part2
Stop

**Figure A-8 FD1_Main_Ingestion_Part2**

### A.2.2 Mitigation Workflow Execution

In parallel to completing the alert investigation process outlined previously, the Main_Detection workflow also passes execution to the Main_Mitigation workflow (see Figure A-7). The Main_Mitigation workflow (Figure A-9) examines the severity of the alert and if it exceeds the set threshold, mitigation COAs are determined and all information related to the alert (e.g., correlated events, results of all Integrity Checks, COAs) is presented to the operator for "human-in-the-loop" decision-making.

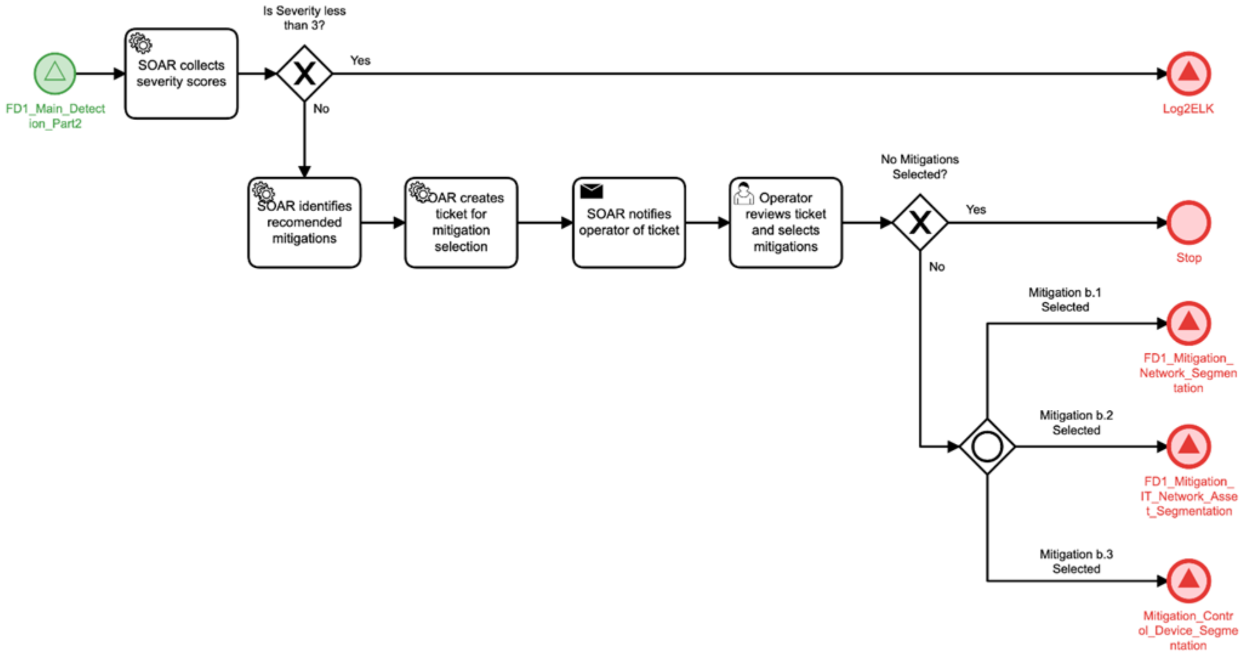
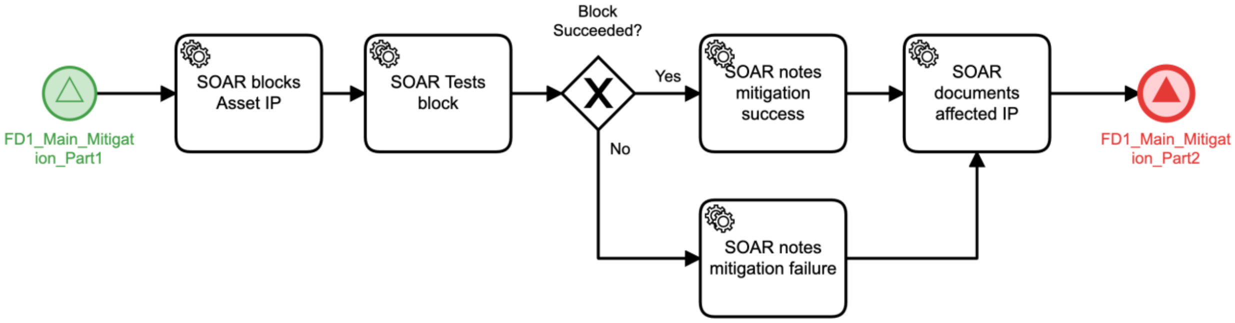

FD1_Main_Detection_Part2
SOAR collects severity scores
Is Severity less than 3?
Yes
No
Log2ELK
SOAR identifies recomended mitigations
SOAR creates ticket for mitigation selection
SOAR notifies operator of ticket
Operator reviews ticket and selects mitigations
No Mitigations Selected?
Yes
No
Stop
Mitigation b.1 Selected
FD1_Mitigation_Network_Segmentation
Mitigation b.2 Selected
FD1_Mitigation_IT_Network_Asset_Segmentation
Mitigation b.3 Selected
Mitigation_Control_Device_Segmentation

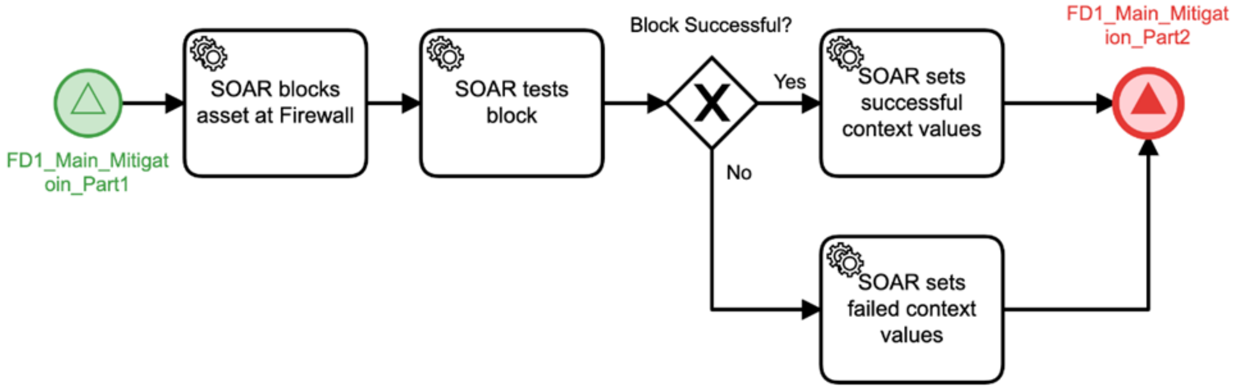
**Figure A-9 FD1_Main_Mitigation_Part1**

The operator can choose to take no action on the alert, in which case execution ends, or can select from the list of pre-approved COAs. When specific COAs are selected by the operator, execution is passed to the corresponding mitigation sub-workflow for automated implementation. Two mitigation workflows were implemented as part of the MOSAICS JCTD. These COA sub-workflows focus on breaking adversarial command and control by implementing firewall rules that isolate the entire control system environment (Figure A-10) or a specific network asset (Figure A-11) from external communications.



FD1_Main_Mitigat ion_Part1
SOAR blocks Asset IP
SOAR Tests block
Block Succeeded?
Yes
No
SOAR notes mitigation success
SOAR documents affected IP
SOAR notes mitigation failure
FD1_Main_Mitigat ion_Part2

**Figure A-10 FD1_Mitigation_Network_Segmentation**



FD1_Main_Mitigat oin_Part1
SOAR blocks asset at Firewall
SOAR tests block
Block Successful?
Yes
No
SOAR sets successful context values
SOAR sets failed context values
FD1_Main_Mitigat ion_Part2

**Figure A-11 FD1_Mitigation_IT_Network_Asset_Segmentation**

Upon completion of the mitigation action, execution is returned to the Main_Mitigation workflow where all automated actions are logged, and the event is closed.

### A.2.3 Information Sharing and Recovery Workflow Execution

Similar to the mitigation workflows, the Information Sharing and Recovery workflows are called based on operator-initiated actions to restore the system to a prior state and/or to share technical information related to an identified threat. The recovery workflow was not fully implemented as part of the MOSAICS JCTD effort, but a templated workflow was used to pass control to the Main_Information_Sharing workflow. This workflow (Figure A-12) collects all alert and Integrity Check data associated with an incident and formats it into a Structured Threat Information Exchange (STIX) bundle for machine-to-machine information sharing. At this point the event is closed, and no further action is taken on the alert.

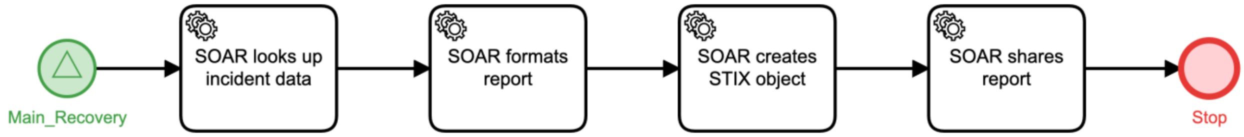


**Figure A-12 Main_Information_Sharing**

## A.3 Full MOSAICS Workflow Representation

The complete end-to-end flow of all the MOSAICS workflows can be seen in Figure A-13. While this flow can be implemented in a variety of ways, this approach allows for easy extensibility as new alerts are developed, data sources are incorporated, pre-approved mitigations are defined, and response actions are added to the system.

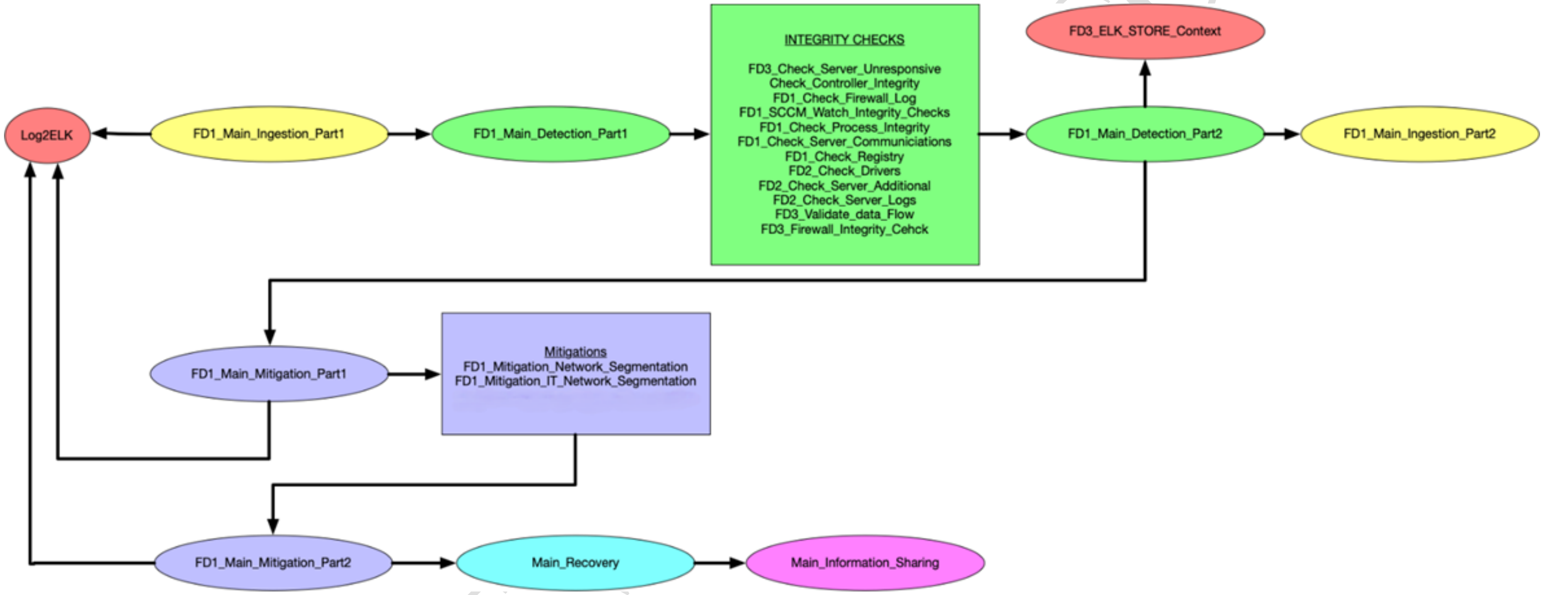

FD3_ELK_STORE_Context
Log2ELK
FD1_Main_Ingestion_Part1
FD1_Main_Detection_Part1
INTEGRITY CHECKS
FD3_Check_Server_Unresponsive
Check_Controller_Integrity
FD1_Check_Firewall_Log
FD1_SCCM_Watch_Integrity_Checks
FD1_Check_Process_Integrity
FD1_Check_Server_Communiciations
FD1_Check_Registry
FD2_Check_Drivers
FD2_Check_Server_Additional
FD2_Check_Server_Logs
FD3_Validate_data_Flow
FD3_Firewall_Integrity_Cehck
FD1_Main_Detection_Part2
FD1_Main_Ingestion_Part2
FD1_Main_Mitigation_Part1
Mitigations
FD1_Mitigation_Network_Segmentation
FD1_Mitigation_IT_Network_Segmentation
FD1_Main_Mitigation_Part2
Main_Recovery
Main_Information_Sharing

**Figure A-13 MOSAICS Workflow Representation**

# APPENDIX B. BEHAVIORAL ALERTING SETS FOR CONTROL SYSTEMS (BAS/CS$^{TM}$)

BAS/CS™

Behavioral Alerting Sets for Control Systems

Behavioral Alerting Sets for Control Systems (BAS/CS$^{TM}$) is a JHU/APL alerting framework. An implementation of BAS/CS$^{TM}$ is an approach toward satisfying the MOSAICS alerting requirements. BAS/CS$^{TM}$ defines a data processing pipeline which firsts normalizes and tags events with BAS/CS$^{TM}$ Event IDs, then proceeds to correlate the events using BAS/CS$^{TM}$ Rules. The tagging and correlation rules defined by BAS/CS$^{TM}$ is intended to be implemented in a commercial Security Information and Event Management (SIEM) capability.

## B.1 BAS/CS$^{TM}$ Events

BAS/CS$^{TM}$ Events are defined as a list of behavior events with standardized tags and names. These events are intended to provide broad groupings to categorize the types of events generated by sensors. The categorization converts sensor vendor specific events into "universal" categories of behavior that are implementation agnostic. This allows for flexibility in the selected sensor capabilities, as the vendor proprietary event generating analytics remain as is, but the resulting events are mapped into a BAS/CS$^{TM}$ Event bucket, standardizing how higher-level analytics can interact with the sensor event data. The BAS/CS$^{TM}$ Events were developed to meet the MOSAICS requirements detailed in Table B-1.

Table B-1: MOSAICS Requirements BAS/CS$^{TM}$ Events

| ID | Requirement |
|---|---|
| **F3.3.1** | MOSAICS shall generate an event whenever any detection criteria (e.g., change in behavior, access/usage rule violation) not captured in the baseline is triggered. |
| **T3.3.3** | MOSAICS shall categorize events with a normalized event tag.<br>Note: The tag is for use in analysis. |
| **T3.3.4** | MOSAICS events shall include the following, at a minimum:<br>• All accompanying data elements used to generate the event<br>• Timestamp of when event created<br>• Normalized event tag<br>• Unique identifier |

There are two main categories of BAS/CS$^{TM}$ Events (BE), Host and Network behaviors (see Table B-2). Host events focus on the events that are generated from within a Host. Network events focus on events generated from network communications.

Table B-2: BAS/CS$^{TM}$ Events

| BE ID | BE Name | BE Description |
|---|---|---|
| **Host Events** | | |
| **ACC01** | NTLM Login Attempt | NTLM login (a pass the hash (PtH) vulnerability) attempt |
| **ACC02** | RDP Authenticated Login Attempt | Remote desktop protocol (RDP) authenticated login attempt |
| **ACC03** | RDP Login | Remote desktop protocol (RDP) (successful) login |
| **ACC04** | Admin Shares | Modification of admin shares settings |
| **ACC05** | New Service | New Service Installed |
| **ACC06** | Scheduled Task | A Scheduled Task was Created |
| **ACC07** | User Created | A new user account has been created |
| **ACC08** | Security Global Group | Security Global Group |
| **ACC09** | Security Local Group | A Member was Added to a Security-Enabled Local Group |
| **ACC10** | Local Group Change | A security-enabled local group was changed |
| **ACC11** | Explicit Login Attempt | New login attempt with explicit credentials |
| **ACC12** | Failed Login Attempt | Unsuccessful login attempt |
| **ACC13** | New Login | New login |
| **ACC14** | Sysvol Write | Write or append to the SYSVOL NTFS volume |
| **LOG01** | Significant Timestamp Difference | Significant timestamp difference in log |
| **LOG02** | | |
| **FIL01** | New File | A new file detected in a monitored file system |
| **PRO01** | Process Change | A process has been created or changed. |
| **PRO02** | AppLocker | AppLocker has blocked a program from executing. |
| **PRO03** | New Shell | A new powershell or command prompt session was created |
| **PRO04** | New Process | A new process was created |
| **PRO05** | Process Stopped | A new process was stopped |
| **PRO06** | Driver Loaded | New kernel driver loaded |
| **PRO07** | Potential Process Injection | Process injection potentially detected |
| **PRO08** | WMI Event Detected | A Windows Management Instrumentation (WMI) event has been detected |
| **PRO09** | Audit Logs Cleared | The security audit logs have been cleared |

| BE ID | BE Name | BE Description |
|---|---|---|
| **PRO10** | System Logs Cleared | System logs have been cleared |
| **PRO11** | Event Logging Stopped | Event logging service has stopped |
| **PRO12** | Process External Reach out | Outgoing remote desktop protocol connection detected |
| **PRO13** | Remote Management Executed Suspicious Process | Suspicious process execution via Windows Management Instrumentation (WMI) was detected. |
| **PRO14** | Remote Management Executed Suspicious Commands | Suspicious process command execution via Windows Management Instrumentation (WMI) was detected. |
| **PRO15** | Remote Service Creation | sc.exe was used to create, modify, or start services on a remote host. |
| **PRO16** | Named Pipe | A named pipe has been created or connected to |
| **USB01** | USB Peripheral Connected | A USB device has connected to the host |
| **USB02** | USB Peripheral Removed | A USB device has disconnected from the host |
| **USB03** | USB Storage Connected | A removable storage device has connected to the host |
| **USB04** | USB Storage Removed | A removable storage device has disconnected from the host |
| **Network Events** | | |
| **IDS01** | Network Conversation Anomaly | A change in the normal conversations between nodes was observed |
| **IDS02** | New Node | A new network node has been established |
| **IDS03** | New Logical Link | A link (communication channel) has been established |
| **IDS04** | OT Write Command | A control system protocol write command was observed |
| **IDS05** | OT Read Command | A control system protocol read command was observed |
| **IDS06** | Function Code Anomaly | An unusual or new function code was observed |
| **IDS07** | Protocol Anomaly | Improper or unusual use of a network protocol was observed |
| **IDS08** | Configuration Change | A change to firmware, logic, or software program has occurred |
| **IDS09** | Hardware Change | Change to serial number, I/O hardware, etc. |
| **IDS10** | Network Interface Change | A change to a MAC or IP address has occurred |
| **IDS11** | External Conversation | A conversation with a node outside of control system boundary has occurred |
| **IDS12** | Network Scanning | Asset or port scanning was observed |

| BE ID | BE Name | BE Description |
|---|---|---|
| **IDS13** | System Elements Not Synchronized | A message with an anomalous time stamp was observed |
| **IDS14** | Device State Change | A mode change or reboot has occurred |
| **IDS15** | Signature Based Alerts | A signature-based alert has been generated |
| **IDS16** | Process Variable Anomaly | A process variable outside normal or expected ranges was observed |
| **NET01** | Link Traffic Increase | An unexpected increase in traffic has occurred. |
| **NET02** | Link Traffic Decrease | An unexpected decrease in traffic has occurred. |
| **NET03** | Link Loss | A communication link has dropped or been lost. |
| **NET04** | Stale Node | A node has stopped communicating |
| **NET05** | Network Scanning | Asset or port scanning has occurred. |
| **NET06** | Network Interface Change | A change to a MAC or IP address has occurred. |

## B.2 BAS/CS$^{TM}$ Alerts

BAS/CS$^{TM}$ Alerts (see Table B-4) are defined as a collection of logical correlations of BAS/CS$^{TM}$ Events. A series of BAS/CS$^{TM}$ Rules are used to determine if the conditions warrant generating a BAS/CS$^{TM}$ Alert. Each BAS/CS$^{TM}$ Rule consists of an Alert Logic statement, which provides the relationship between the BAS/CS$^{TM}$ Events using AND (&&) and OR (||) expressions. Each of these logical expressions are used to query the BAS/CS$^{TM}$ Event data in a SIEM, and if the logical expression returns True, for the given time range and aggregation field (typically the event source hostname), then a BAS/CS$^{TM}$ Alert is generated. The BAS/CS$^{TM}$ Alerts were developed to meet the MOSAICS requirements detailed in Table B-3.

Table B-3: MOSAICS Requirements BAS/CS$^{TM}$ Alerts

| ID | Requirement |
|---|---|
| **F4.1.1** | MOSAICS shall analyze events. |
| **T4.1.1.1** | MOSAICS shall correlate events across assets, network communications, and time for analysis. |
| **T4.1.1.2** | MOSAICS shall generate an alert based on predefined threat patterns of behavior. |

Table B-4: BAS/CS$^{TM}$ Alerts

| Alert ID | Alert Name | Alert Description |
|---|---|---|

| | | |
|---|---|---|
| BAS.2.1 | Unusual Account Activity | A new shell process has been created or AppLocker has warned against the execution of a script or installer (.msi) file. A user may be attempting to execute malicious commands, scripts, or binaries. |
| BAS.2.2 | Unusual Account Activity (Potential Privilege Escalation) | One or more suspicious actions have been identified: installing a new Windows service, creating a scheduled task, creating a new user, adding a member to a security-enabled group, or modifying a security-enabled group. This may indicate a user is attempting to gain elevated privileges. |
| BAS.2.3 | Unusual Account Activity (Potential Privilege Escalation) (Enriched) | One or more suspicious actions have been identified: installing a new Windows service, creating a scheduled task, creating a new user, adding a member to a security-enabled group, or modifying a security-enabled group. Additionally, a user has attempted to logon using explicit credentials. This may indicate a user is attempting to gain elevated privileges and may have scheduled a task or used the "RUNAS" command. |
| BAS.3 | Unusual Process Detected | A process has been detected that is not within the list of known, expected processes. An adversary may be executing malicious code on the system. |
| BAS.4 | Suspicious Process Termination | A process has been terminated that is not within the list of known, expected processes. |
| BAS.5 | Irregular Audit Log Event | One or more audit logs have been cleared or stopped, or contain significant timestamp differences. An attacker may be attempting to evade detection. |
| BAS.6 | Suspicious Kernel Driver Installed | A suspicious kernel driver has been installed. |
| BAS.7 | Network Enumeration activity | A device is perceived to be communicating with other devices in an attempt to enumerate details about the endpoint devices. |
| BAS.8.1 | Unexpected OT Command and Control | Unexpected behavior of an HMI, OPC, or control server affecting controllers. HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds. Expected changes to controllers are not appearing on controllers. |
| BAS.8.2 | Unexpected OT Command and Control (Shell Activity) | Signs of process injection have been detected and changes have been made to your network. An attacker may be attempting to establish command and control. |
| BAS.8.3 | Unexpected OT Command and Control (Process Injection Focused) | Signs of process injection have been detected and changes have been made to your network. An attacker may be attempting to establish command and control using process injection. |
| BAS.9 | Loss of Communication | One or more devices on your network are no longer communicating. A denial-of-view attack may be affecting devices in order to mask an attacker's activities. |
| BAS.11 | Unusual Control System Traffic | An unusual Internet protocol (IP) address or an unusual port, protocol, or service (from a known IP address) is attempting to communicate with the control system. |
| BAS.19 | Unexpected Device Changes | A change has been made to the control equipment configured settings (Ladder Logic/Code Configurations, Firmware, Set Points, Hardware, etc.). Control Equipment settings should only be changed while in a maintenance window with approval. |

|  |  |  |
|---|---|---|
| BAS.20 | Remote OT Command Activity | A remote connection has been established to a device on the control system network. This connection is engaging in OT command and control activity, attempting to impact the physical control system. |
| BAS.24 | Unusually High Network Traffic | The network is experiencing higher-than-usual traffic. This may be due to network scanning or a denial-of-service attack aimed to disrupt operations. |
| BAS.25 | Unusual Decrease in Network Traffic | The normal flow of control traffic appears slower, sluggish, or there is less traffic than normal (polling cycles not executing for example). |
| BAS.26 | Unexpected Connection to External or Unknown IPs | An control system field controller is communicating with an unknown device or machine. |
| BAS.27 | Potential Lateral Movement | Recent remote login attempts or other suspicious network activity have been detected. An unexpected process has also been identified. An attacker may be conducting lateral movement on the network. |
| BAS.28.1 | Potentially Malicious Command & Control Activity | File creation, suspicious process, and network events have been identified. This may indicate that an attacker is attempting to establish command and control using a malicious process. |
| BAS.28.2 | Potentially Malicious Command & Control Activity (Shell Activity) | Signs of process injection have been detected and changes have been made to your network. An attacker may be attempting to establish a command and control presence. |
| BAS.28.3 | Potentially Malicious Command & Control Activity (Process Injection Focused) | Signs of process injection have been detected and changes have been made to your network. An attacker may be attempting to establish a command and control presence. |
| BAS.29 | Suspected Sysvol Admin Share Lateral Movement | An adversary may be using the Sysvol admin share to move laterally within the network. |
| BAS.30 | Potentially Malicious PowerShell or Command Shell Activity | A new remote connection or shell has been created and may have been used to modify network settings or create a new process, file, or network node. |
| BAS.31 | Potentially Malicious Privilege Escalation Activity | A new user has been created and a user has been added to a global security-enabled group. This may indicate a privilege escalation attempt. |
| BAS.32.1 | Potentially Malicious Persistence Established | A new file has been created, and a new scheduled task has been created. This may indicate that a malicious user is attempting to establish persistence. |
| BAS.32.2 | Potentially Malicious Persistence Established (Process) | A suspicious process, shell usage, and suspicious OT network function requests have been detected. An adversary may be attempting to gain persistence within your system. |

| | | |
|---|---|---|
| BAS.34 | Potentially Malicious WMI Activity | A suspicious Windows Management Instrumentation (WMI) event has been detected. An attacker may be attempting to escalate privileges or gain persistence within your system. |
| BAS.35 | WMI Remote Execution (Destination) | A suspicious remote Windows Management Instrument (WMI) event has been detected. An attacker may be trying to gain persistence or escalate privilege via remote command execution. |
| BAS.36 | Malicious Network Behavior Signature | A signature-based detection has been triggered from a network intrusion detection system. A signature-based detection is very likely indicating malicious behavior within the network. |

## B.3 Implementing BAS/CS$^{TM}$

To implement BAS/CS$^{TM}$ Events, the detection functional requirements listed in Table B-5, and the associated technical requirements must be implemented. These requirements define what events need to be detected, and lay the foundation to having event data which can be tagged with BAS/CS$^{TM}$ Event IDs.

Table B-5: BAS/CS$^{TM}$ Requirement Dependencies

| ID | Requirement |
|---|---|
| **F3.1.1** | MOSAICS shall continuously monitor network communication within the protected enclave. |
| **F3.1.2** | MOSAICS shall continuously monitor the status of protected enclave assets. |
| **F3.2.1** | MOSAICS shall detect changes to the configuration of protected enclave assets. |
| **F3.2.2** | MOSAICS shall detect abnormal behavior of protected enclave assets. |
| **F3.2.3** | MOSAICS shall detect malicious indicators on protected enclave assets. |
| **F3.2.4** | MOSAICS shall detect changes to the configuration of protected enclave network communications. |
| **F3.3.5** | MOSAICS shall detect abnormal behavior of the protected enclave network communications. |
| **F3.3.6** | MOSAICS shall detect malicious indicators on the protected enclave network communications. |

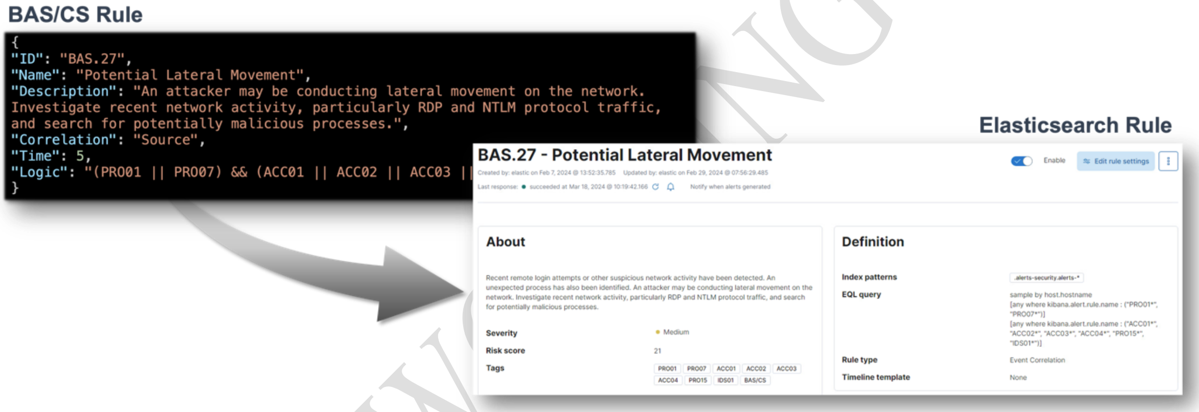
The Tagging of the BAS/CS$^{TM}$ Events may be implemented as a part of several capabilities. One option is to have the endpoint sensors implement the BAS/CS$^{TM}$ Event tagging, so all events generated have the BAS/CS$^{TM}$ Event ID (BE ID) as an event field. If the sensor does not implement the tagging, then an event aggregation capability could implement the tagging with a lookup table pipeline. This pipeline would inspect each event received, compare the event details to a lookup table and add a new BE ID field with the proper BE ID tagged. If no event aggregator is in use, the SIEM could have a pre-indexing processor to implement the same method as the event aggregator, but within the SIEM.

BAS/CS$^{TM}$ Rules are implemented within the SIEM or analytics platform with access to the common events. The BAS/CS$^{TM}$ Rules are defined in JSON, allowing them to be converted into the custom formats each SIEM needs to ingest and implement the rule. BAS/CS™ Rules require all the BAS/CS™ Event requirements to be met, in addition to the event generation requirements in Table B-6.

Table B-6: BAS/CS™ Requirement Dependencies

| ID | Requirement |
|---|---|
| **T3.3.1** | MOSAICS shall store events in a common data repository. |
| **T3.3.2** | MOSAICS shall generate an event within 1 minute of the activity resulting in the event. |

Figure B-1 shows an example of how the BAS/CS™ Rule JSON can be implemented in Elasticsearch. This implementation was accomplished with a custom script which read the BAS/CS™ Rule JSON file, and renamed the Fields, and converted the logic into the syntax expected by Elasticsearch. The script then exported the new rule format as a ndjson file, which is the file type Elasticsearch expects for rule imports. This file can then be manually imported into the Elasticsearch instance, or loaded with API calls.



```
{
"ID": "BAS.27",
"Name": "Potential Lateral Movement",
"Description": "An attacker may be conducting lateral movement on the network.
Investigate recent network activity, particularly RDP and NTLM protocol traffic,
and search for potentially malicious processes.",
"Correlation": "Source",
"Time": 5,
"Logic": "(PRO01 || PRO07) && (ACC01 || ACC02 || ACC03 ||
}
```

BAS.27 - Potential Lateral Movement

Created by: elastic on Feb 7, 2024 @ 13:52:35.785    Updated by: elastic on Feb 29, 2024 @ 07:56:29.485

Last response: ● succeeded at Mar 18, 2024 @ 10:19:42.166    Notify when alerts generated

Enable    Edit rule settings

About

Recent remote login attempts or other suspicious network activity have been detected. An unexpected process has also been identified. An attacker may be conducting lateral movement on the network. Investigate recent network activity, particularly RDP and NTLM protocol traffic, and search for potentially malicious processes.

| | |
|---|---|
| Severity | ● Medium |
| Risk score | 21 |
| Tags | PRO01 PRO07 ACC01 ACC02 ACC03 ACC04 PRO15 IDS01 BAS/CS |

Definition

| | |
|---|---|
| Index patterns | .alerts-security.alerts-* |
| EQL query | sample by host.hostname<br>[any where kibana.alert.rule.name : ("PRO01*", "PRO07*")]<br>[any where kibana.alert.rule.name : ("ACC01*", "ACC02*", "ACC03*", "ACC04*", "PRO15*", "IDS01*")] |
| Rule type | Event Correlation |
| Timeline template | None |

Figure B-1: BAS/CS™ Rule Converted in the Elastic Security Rule

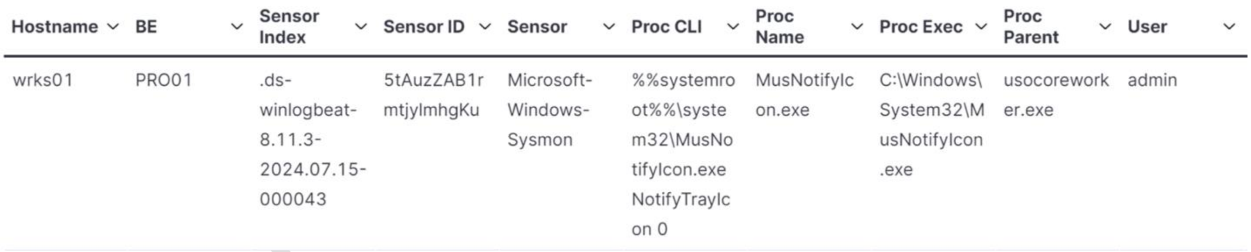
# APPENDIX C. OPERATOR VISUALIZATION EXAMPLES

This Appendix contains example screenshots for the implementation of MOSAICS visualization requirements. These are examples only and do not prescribe this particular implementation.

The first example, Figure C-1, is an event visualization in table form. The columns include the Behavioral Alert Set for Control Systems (BAS/CS™) event identifier (see Appendix B) (BE column), the sensor that detected the event (Sensor Index and Sensor ID columns), additional information about the process that triggered the event (Proc CLI, Name, Exec, and Parent columns), and information about the user (User column). Each of the columns are both filterable and sortable (ascending/descending). This visualization is an example related to requirements in Table C-1.

**Table C-1: MOSAICS Event Visualization Requirements Example**

| ID | Requirement |
|---|---|
| **F5.1.1** | MOSAICS shall provide the capability to visualize detected events. |
| **T5.1.1.2** | MOSAICS shall allow a user to perform sorts on event data. |
| **T5.1.1.3** | MOSAICS shall allow a user to perform filtering on event data. |
| **F5.2.1** | MOSAICS shall provide the capability to visualize the protected enclave status |
| **T5.2.1.1** | MOSAICS shall allow the user to view logs, events and alerts. |



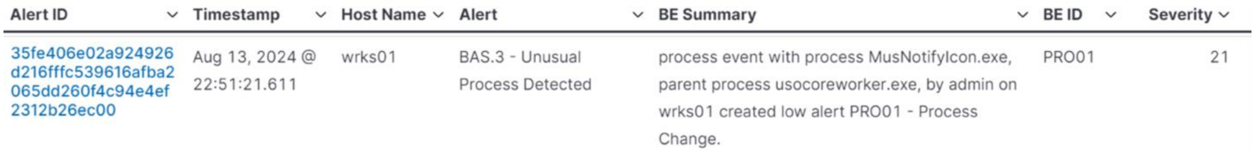
| Hostname | BE | Sensor Index | Sensor ID | Sensor | Proc CLI | Proc Name | Proc Exec | Proc Parent | User |
|---|---|---|---|---|---|---|---|---|---|
| wrks01 | PRO01 | .ds-winlogbeat-8.11.3-2024.07.15-000043 | 5tAuzZAB1rmtjylmhgKu | Microsoft-Windows-Sysmon | %%systemroot%%\system32\MusNotifyIcon.exe NotifyTrayIcon 0 | MusNotifyIcon.exe | C:\Windows\System32\MusNotifyIcon.exe | usocoreworker.exe | admin |

**Figure C-1. MOSAICS Event Visualization in a Table Format**

Figure C-2 is an example showing how the alerts are displayed in table format. Each alert is given a unique identifier (Alert ID), the timestamp at which the alert was created, the affected host(s), a description of the alert, a description of the events that caused the alert (BE Summary), and a severity level. Each of the columns in the Figure C-2 screenshot are both filterable and sortable for investigative purposes. This visualization is an example that pertains to the requirements in Table C-2.

### Table C-2: Alert Table Visualization Requirements

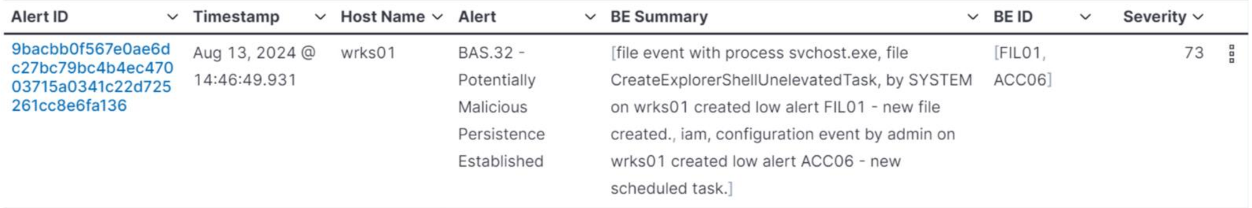
| ID | Requirement |
|---|---|
| **F5.2.1** | MOSAICS shall provide the capability to visualize the protected enclave status |
| **T5.2.1.1** | MOSAICS shall allow the user to view logs, events and alerts. |
| **F5.3.2** | MOSAICS shall provide the capability to visualize alerts. |
| **T5.3.2.1** | MOSAICS shall have the capability to visualize any alert |
| **T5.3.2.2** | MOSAICS shall have the capability to see correlated events for a given alert. |
| **T5.3.2.4** | MOSAICS shall provide the ability to search, sort, and filter alerts by data attributes. |



| Alert ID | Timestamp | Host Name | Alert | BE Summary | BE ID | Severity |
|---|---|---|---|---|---|---|
| 35fe406e02a924926d216fffc539616afba2065dd260f4c94e4ef2312b26ec00 | Aug 13, 2024 @ 22:51:21.611 | wrks01 | BAS.3 - Unusual Process Detected | process event with process MusNotifyIcon.exe, parent process usocoreworker.exe, by admin on wrks01 created low alert PRO01 - Process Change. | PRO01 | 21 |

**Figure C-2. MOSAICS Alert Table Visualization**

The example shown in Figure C-3 highlights how an alert can be a result of multiple events. Here, an alert was a result of event IDs ACC06 and FIL01, since the events that occurred were a new scheduled task and a new file created. The combination of these events became an alert for a potential malicious persistence being established.



| Alert ID | Timestamp | Host Name | Alert | BE Summary | BE ID | Severity |
|---|---|---|---|---|---|---|
| 9bacbb0f567e0ae6dc27bc79bc4b4ec47003715a0341c22d725261cc8e6fa136 | Aug 13, 2024 @ 14:46:49.931 | wrks01 | BAS.32 - Potentially Malicious Persistence Established | [file event with process svchost.exe, file CreateExplorerShellUnelevatedTask, by SYSTEM on wrks01 created low alert FIL01 - new file created., iam, configuration event by admin on wrks01 created low alert ACC06 - new scheduled task.] | [FIL01, ACC06] | 73 |

**Figure C-3. MOSAICS Alerts as a Result of Multiple Events**

The example in Figure C-4 shows a breakdown by workstation and alerts for the protected enclave. The operator is able to digest what issues are plaguing which assets in an easily identifiable manner. In addition, there is a sorted table on the right of the visualization that provides the totals for each type of alert across all assets as a way to understand the impacts to the enclave. This visualization is an example related to the requirements in Table C-3.

### Table C-3: MOSAICS Incident Breakdown Requirements

| ID | Requirement |
|---|---|
| **F5.2.1** | MOSAICS shall provide the capability to visualize the protected enclave status |
| **T5.2.1.1** | MOSAICS shall allow the user to view logs, events and alerts. |

| ID | Requirement |
|---|---|
| **T5.2.1.2** | MOSAICS shall provide the capability to display which asset of the protected enclave have been affected by alerts and events |
| **F5.3.2** | MOSAICS shall provide the capability to visualize alerts. |
| **T5.3.2.7** | MOSAICS shall perform trending and charting of alert/incident data. |

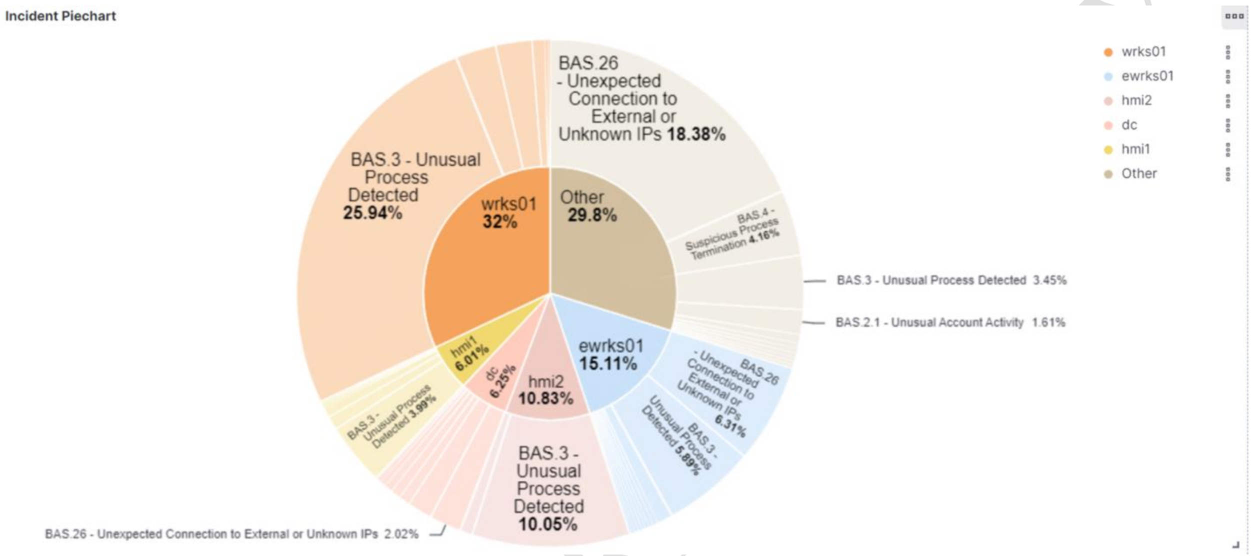
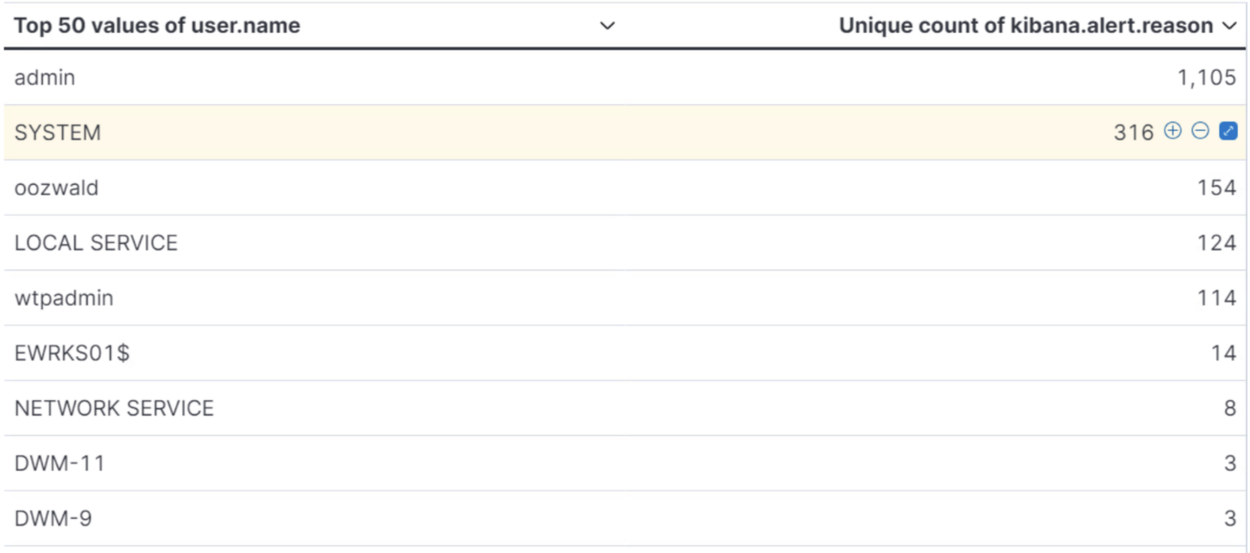


**Figure C-4. MOSAICS Incident Breakdown Visualization**

MOSAICS has the capability to aggregate each host for the processes and the users that have logged onto the machine. In addition, MOSAICS has the capability to keep track of which user is logged into an asset, so when an alert occurs, it can be correlated for where the potential security issues may be coming from. This visualization (Figure C-5) is an example for a single asset and is related to the requirements in Table C-4.

**Table C-4: MOSAICS Asset User Table Requirement**

| ID | Requirement |
|---|---|
| **F5.2.1** | MOSAICS shall provide the capability to visualize the protected enclave status |
| **T5.2.1.4** | MOSAICS shall provide the capability to display the user accounts logged in to assets monitored by MOSAICS. |



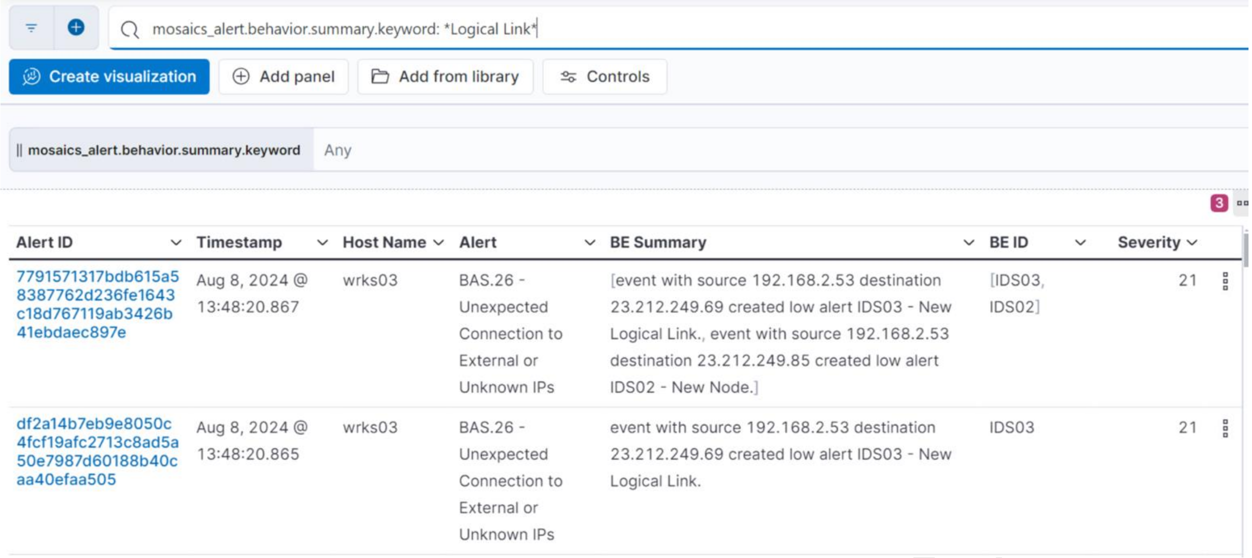
| Top 50 values of user.name | Unique count of kibana.alert.reason |
|---|---|
| admin | 1,105 |
| SYSTEM | 316 ⊕ ⊖ |
| oozwald | 154 |
| LOCAL SERVICE | 124 |
| wtpadmin | 114 |
| EWRKS01$ | 14 |
| NETWORK SERVICE | 8 |
| DWM-11 | 3 |
| DWM-9 | 3 |

**Figure C-5. MOSAICS Asset User Account Table**

MOSAICS is able to search alerts to assist the operator examining alerts. In the example shown in Figure C-6, MOSAICS is able to search using wildcards in order to find specific strings in the Summary field of the Alert table. For each example alert noted, the phrase "Logical Link" can be found. In this example, MOSAICS has the capability to either search for the entire matching text or just a specific phrase the operator is interested in. This search, and the table, is an example related to the requirements in Table C-5.

**Table C-5: MOSAICS Searching Capability Requirement**

| ID | Requirement |
|---|---|
| **F5.3.2** | MOSAICS shall provide the capability to visualize alerts. |
| **T5.3.2.4** | MOSAICS shall provide the ability to search, sort, and filter alerts by data attributes. |


mosaics_alert.behavior.summary.keyword: *Logical Link*
Create visualization
Add panel
Add from library
Controls
|| mosaics_alert.behavior.summary.keyword
Any
3

| Alert ID | Timestamp | Host Name | Alert | BE Summary | BE ID | Severity |
|---|---|---|---|---|---|---|
| 7791571317bdb615a58387762d236fe1643c18d767119ab3426b41ebdaec897e | Aug 8, 2024 @ 13:48:20.867 | wrks03 | BAS.26 - Unexpected Connection to External or Unknown IPs | [event with source 192.168.2.53 destination 23.212.249.69 created low alert IDS03 - New Logical Link., event with source 192.168.2.53 destination 23.212.249.85 created low alert IDS02 - New Node.] | [IDS03, IDS02] | 21 |
| df2a14b7eb9e8050c4fcf19afc2713c8ad5a50e7987d60188b40caa40efaa505 | Aug 8, 2024 @ 13:48:20.865 | wrks03 | BAS.26 - Unexpected Connection to External or Unknown IPs | event with source 192.168.2.53 destination 23.212.249.69 created low alert IDS03 - New Logical Link. | IDS03 | 21 |

**Figure C-6. MOSAICS Searching Capability**

# APPENDIX D. ACRONYMS

| | |
|---|---|
| ACI TTP | Cyber Industrial Control System Tactics, Techniques, and Procedures |
| ADS | Alternate Data Streams |
| AI | Artificial Intelligence |
| API | Application Programming Interfaces |
| ARP | Address Resolution Protocol |
| BAS/CS™ | Behavioral Alert Set for Control Systems |
| BE | BAS/CS™ Event |
| COA | Course of Action |
| COTS | Commercial off the Shelf |
| DCS | Distributed Control Systems |
| DHCP | Dynamic Host Configuration Protocol |
| DoD | Department of Defense |
| ELK | Elastic Search, Logstash, and Kibana |
| FTP | File Transfer Protocol |
| GOTS | Government off the Shelf |
| IACD | Integrated Adaptive Cyber Defense |
| ICS | Industrial Control System |
| ID | Identifier |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| ISA | Interconnection Security Agreement |
| IT | Information Technology |
| JCTD | Joint Capability Technology Demonstration |

| | |
|---|---|
| JHU/APL | The Johns Hopkins University Applied Physics Laboratory |
| LMHOSTS | LAN Manager Hosts |
| MAC Address | Media Access Control Address |
| ML | Machine Learning |
| MOSAICS | More Situational Awareness for Industrial Control Systems |
| OS | Operating System |
| OT | Operational Technology |
| PLC | Programmable Logic Controller |
| RBAC | Role Based Access Control |
| RDP | Remote Desktop Protocol |
| SCADA | Supervisory Control and Data Acquisition |
| SCCM | System Center Configuration Manager |
| SIEM | Security Information and Event Management |
| SOAR | Security Orchestration and Automated Response |
| SPAN | Switched Port Analyzer |
| SSH | Secure Shell |
| STIX | Structured Threat Information Exchange |
| TTP | Tactics, Techniques, and Procedures |
| USB | Universal Serial Bus |
| WMI | Windows Management Instrumentation |