JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

MOSAICS Spiral 0 Reference Implementation

Harley Parkes, IACD Lead

26 March 2019

What is IACD?

IACD *defines a <u>strategy</u> and <u>framework</u> to adopt an extensible, adaptive, COTS-based approach*

IACD
Accelerating the Speed and Scale of Cyber Defense

Plug-and-Play

Interoperability & Automation

Bring Your Own Enterprise

Information Sharing

Integrated Adaptive Cyber Defense:
an ecosystem because there are no silver bullets

MOSAICS
OV-1

ICS Protection

Facilities Engineer

Cyber Defender

Industrial Control Systems (ICS)

Joint Warfighter Operations

Operational Cyber Defense Capabilities

Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

Smart Integration of Automation

Mission Assurance

Water

Electric Grid

Fuel

Building /Plant

Protect Critical Infrastructure Control Systems from Cyber Attacks

Spiral 0 RI - Purpose

- NSA-sponsored Proof of Concept effort
- Apply IACD concepts to ICS/SCADA
- Prove ability to automate aspects of the ACI TTP
- Demonstrate capability early in program
- Capture lessons learned for application to MOSAICS

Spiral 0 RI – Design Constraints & Limitations

- All work done within a single 90-day Spiral timeframe
- Attempted to use as little custom code development as possible
- Selected security products **may** differ from those used in MOSAICS
  - Example: No robust end-point solution utilized.
- No attempt to replicate selected NAVFAC environment at this time
- Operational constraints not known/considered
- Recovery/Reintegration/Data Sharing aspects not addressed

Spiral 0 RI – Required Capabilities

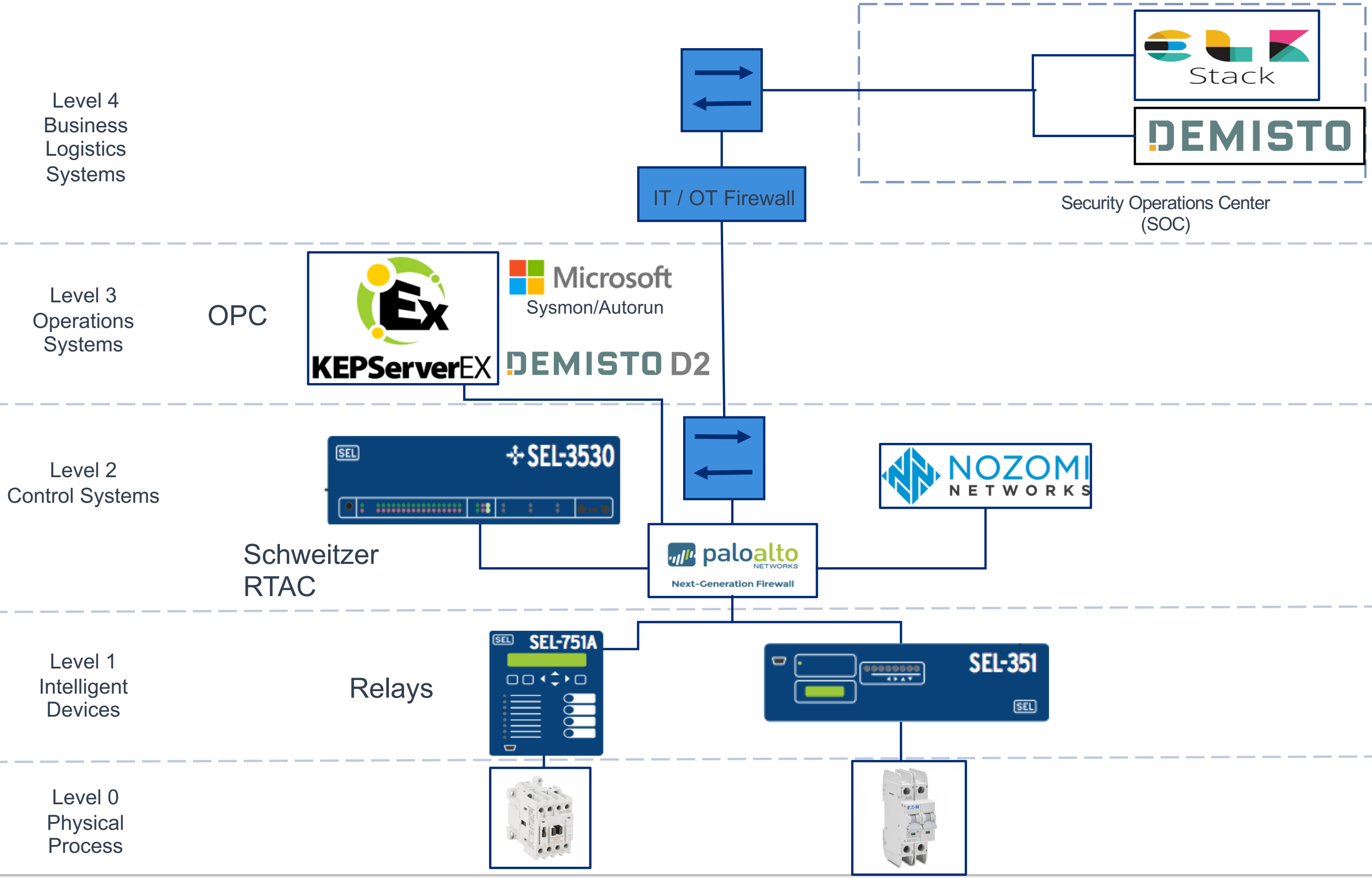
DEMISTO - Security Orchestration

Stack - Security Information Event Management (SIEM)

NOZOMI NETWORKS - Network-based Intrusion Detection (ICS Capable)

Microsoft Sysmon/Autorun - Process Change Detection/End-point Data Access

paloalto NETWORKS Next-Generation Firewall - Next Generation Firewall



Level 4
Business
Logistics
Systems

IT / OT Firewall

Stack

DEMISTO

Security Operations Center
(SOC)

Level 3
Operations
Systems

OPC

KEPServerEX

Microsoft
Sysmon/Autorun

DEMISTO D2

Level 2
Control Systems

SEL
SEL-3530

Schweitzer
RTAC

paloalto
NETWORKS
Next-Generation Firewall

NOZOMI
NETWORKS

Level 1
Intelligent
Devices

Relays

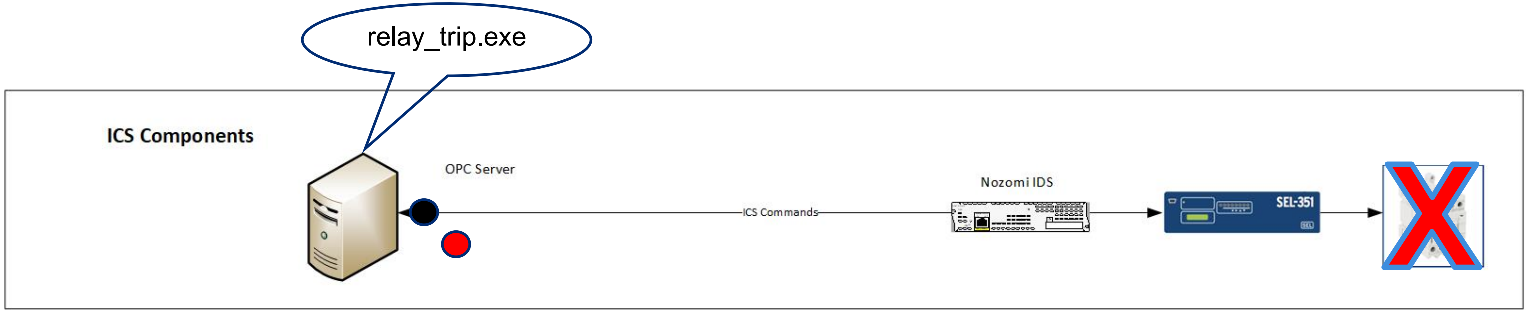
SEL
SEL-751A

SEL-351
SEL

Level 0
Physical
Process

Attack Scenario - Malicious Process Detection and Response

This Reference Implementation addresses the response if an attacker was on a supervisory system and started a process for generating and sending malicious commands to ICS components to disrupt power distribution.



ACI TTP Execution

Detect: Irregular Process Found (A.2.3)
Unexpected Behavior for OPC (A.2.8)

Analyze: Process Integrity Check (A.3.2.1)
Unauthorized User Activity (A.3.2.3)
Server Comms Check (A.3.2.4)
Server Registry Check (A.3.2.6)
Firewall Log Check (A.3.2.11)

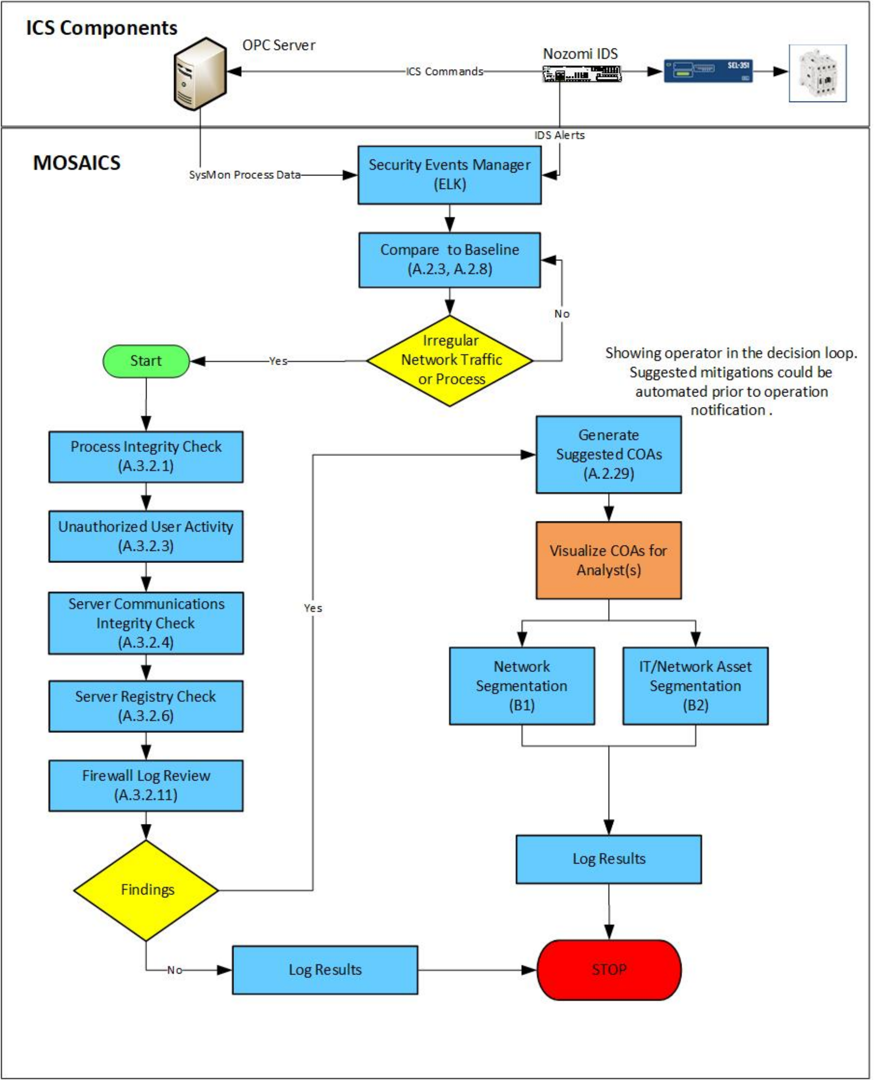
Visualize: Manual, human-in-the-loop

Decide: Manual, human-in-the-loop

Mitigate: Network Segmentation (B1)
IT Asset Segmentation (B2)

Recover: Not Included

Share: Not Included



ICS Components

OPC Server

ICS Commands

Nozomi IDS

IDS Alerts

MOSAICS

SysMon Process Data

Security Events Manager (ELK)

Compare to Baseline (A.2.3, A.2.8)

Irregular Network Traffic or Process

No

Yes

Start

Showing operator in the decision loop. Suggested mitigations could be automated prior to operation notification .

Process Integrity Check (A.3.2.1)

Unauthorized User Activity (A.3.2.3)

Server Communications Integrity Check (A.3.2.4)

Server Registry Check (A.3.2.6)

Firewall Log Review (A.3.2.11)

Findings

Yes

No

Generate Suggested COAs (A.2.29)

Visualize COAs for Analyst(s)

Network Segmentation (B1)

IT/Network Asset Segmentation (B2)

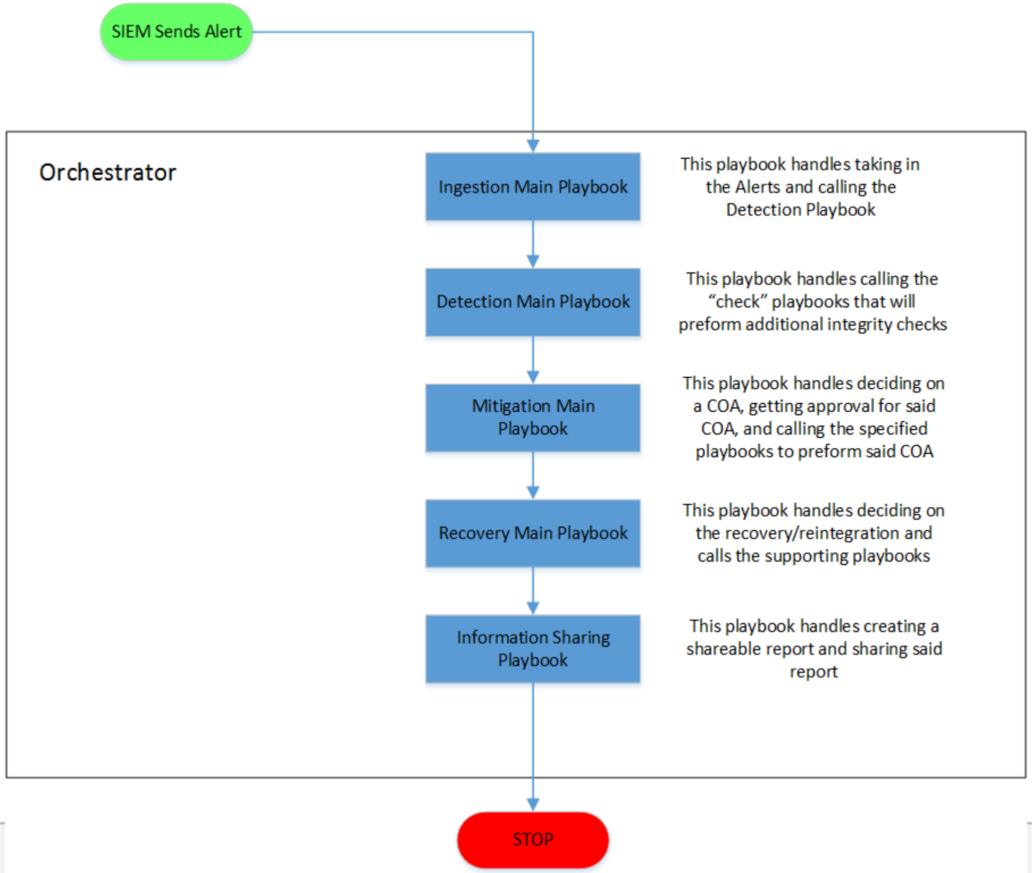
Log Results

Log Results

STOP

MOSAICS Playbook Hierarchy Design

The following addresses how playbooks will be designed in order to support future extensability



SIEM Sends Alert

Orchestrator

Ingestion Main Playbook

This playbook handles taking in the Alerts and calling the Detection Playbook

Detection Main Playbook

This playbook handles calling the "check" playbooks that will preform additional integrity checks

Mitigation Main Playbook

This playbook handles deciding on a COA, getting approval for said COA, and calling the specified playbooks to preform said 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

STOP

Demonstration

Spiral 0 RI – Lessons Learned

- Creation of known-good baseline critical to success
  - Baseline storage & updating are important considerations
- IT Orchestration platform worked well in ICS space (vs OT orchestration platform)
- Hierarchal playbook design highly flexible/expandable/reusable
  - Integrations may not be reusable
  - RESTful API’s are vital to successful integration
- Robust end-point sensor required for TTP execution
- ICS network sensors w/deep packet inspection essential
- ACI TTP checks can be expanded upon (e.g. registry integrity)
- Automation of some checks require additional research (e.g. controller integrity)
- TTP Mitigations are physical actions, need to consider virtual equivalents

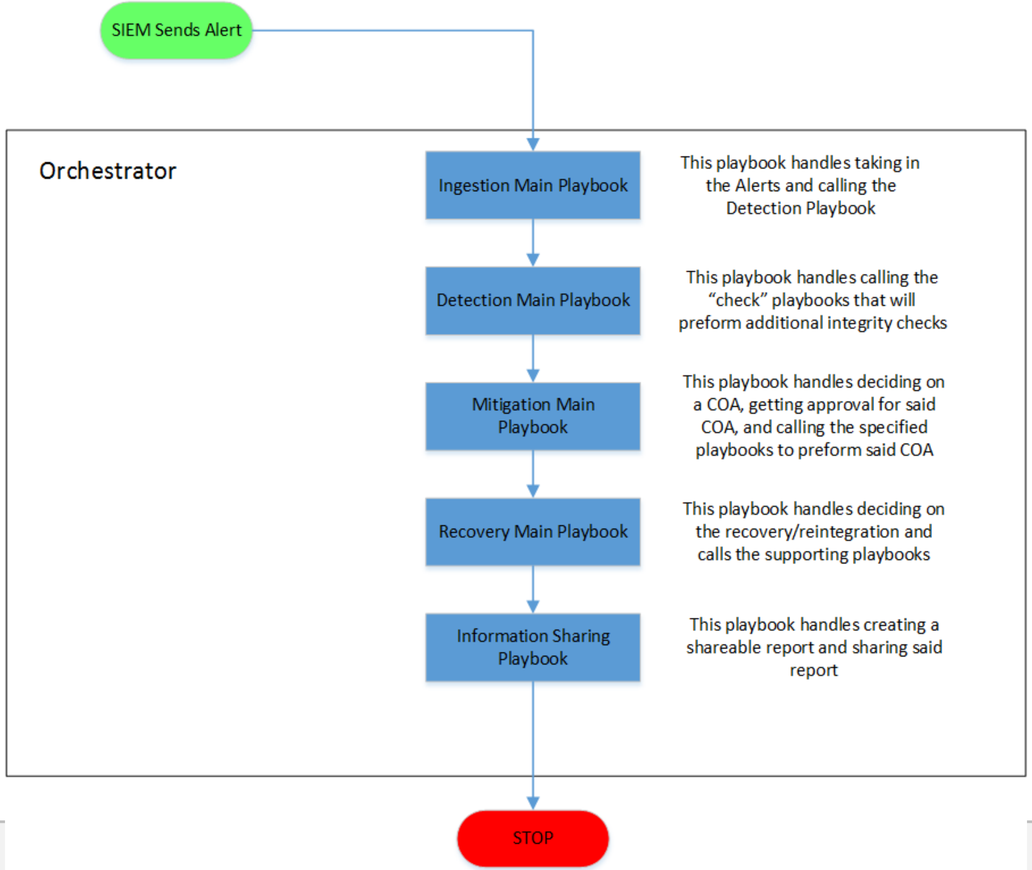
APL

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY

MOSAICS Playbook Hierarchy Design

The following addresses how playbooks will be designed in order to support future extensability



This playbook handles taking in the Alerts and calling the Detection Playbook

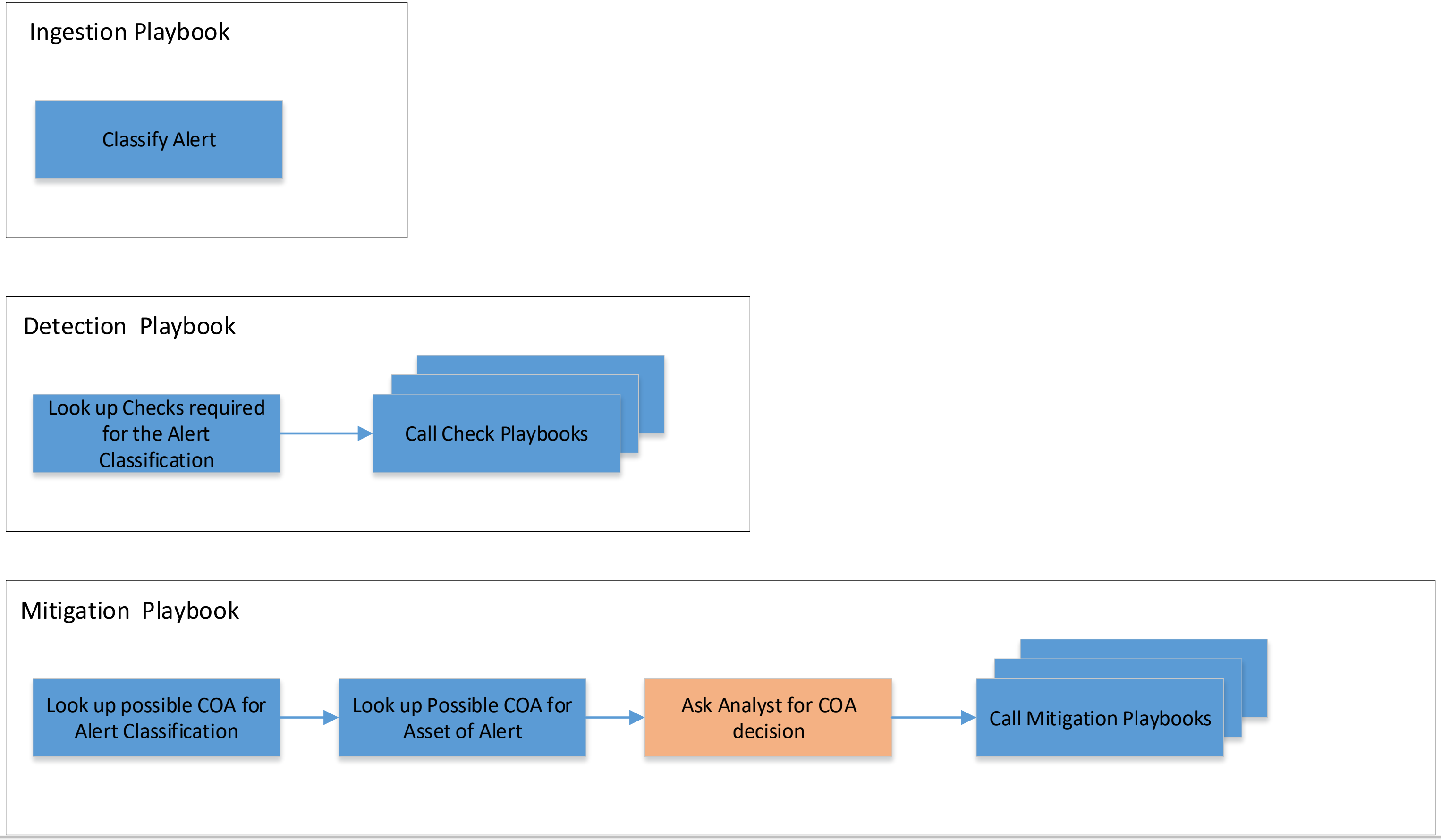
This playbook handles calling the "check" playbooks that will preform additional integrity checks

This playbook handles deciding on a COA, getting approval for said COA, and calling the specified playbooks to preform said COA

This playbook handles deciding on the recovery/reintegration and calls the supporting playbooks

This playbook handles creating a shareable report and sharing said report

MOSAICS Playbook Breakdown



Ingestion Playbook

Classify Alert

Detection Playbook

Look up Checks required for the Alert Classification

Call Check Playbooks

Mitigation Playbook

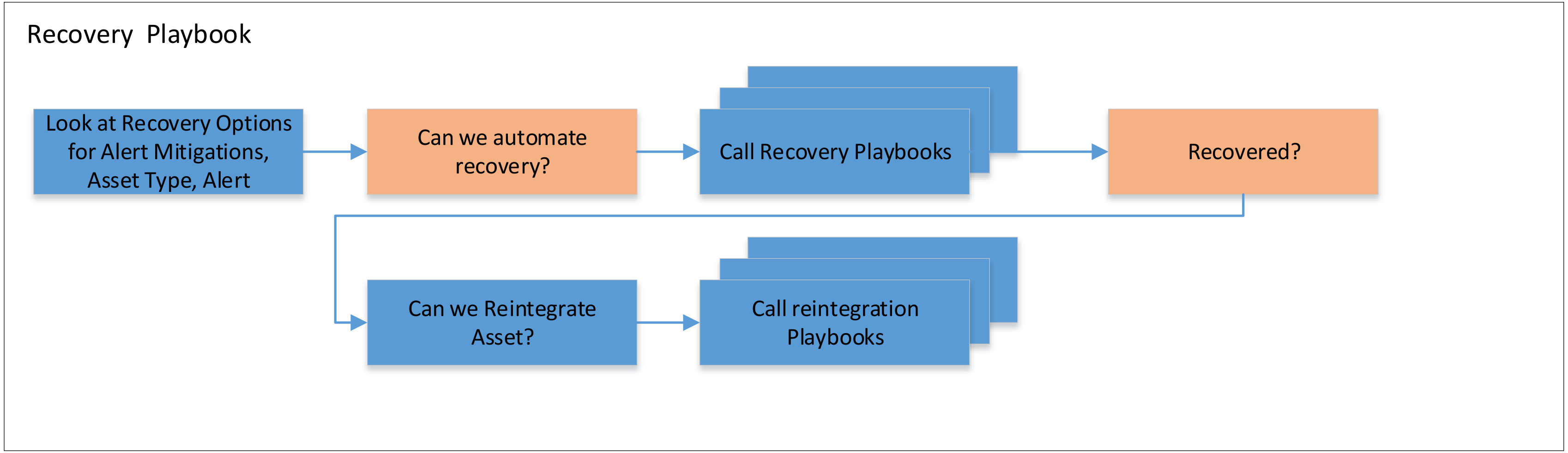
Look up possible COA for Alert Classification

Look up Possible COA for Asset of Alert

Ask Analyst for COA decision

Call Mitigation Playbooks

MOSAICS Playbook Breakdown (cont.)



Recovery Playbook

Look at Recovery Options for Alert Mitigations, Asset Type, Alert

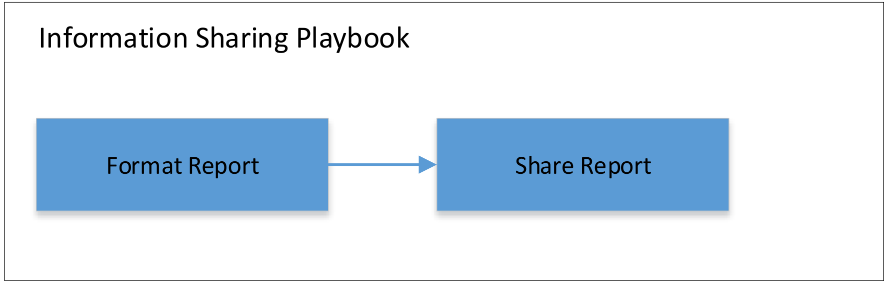
Can we automate recovery?

Call Recovery Playbooks

Recovered?

Can we Reintegrate Asset?

Call reintegration Playbooks

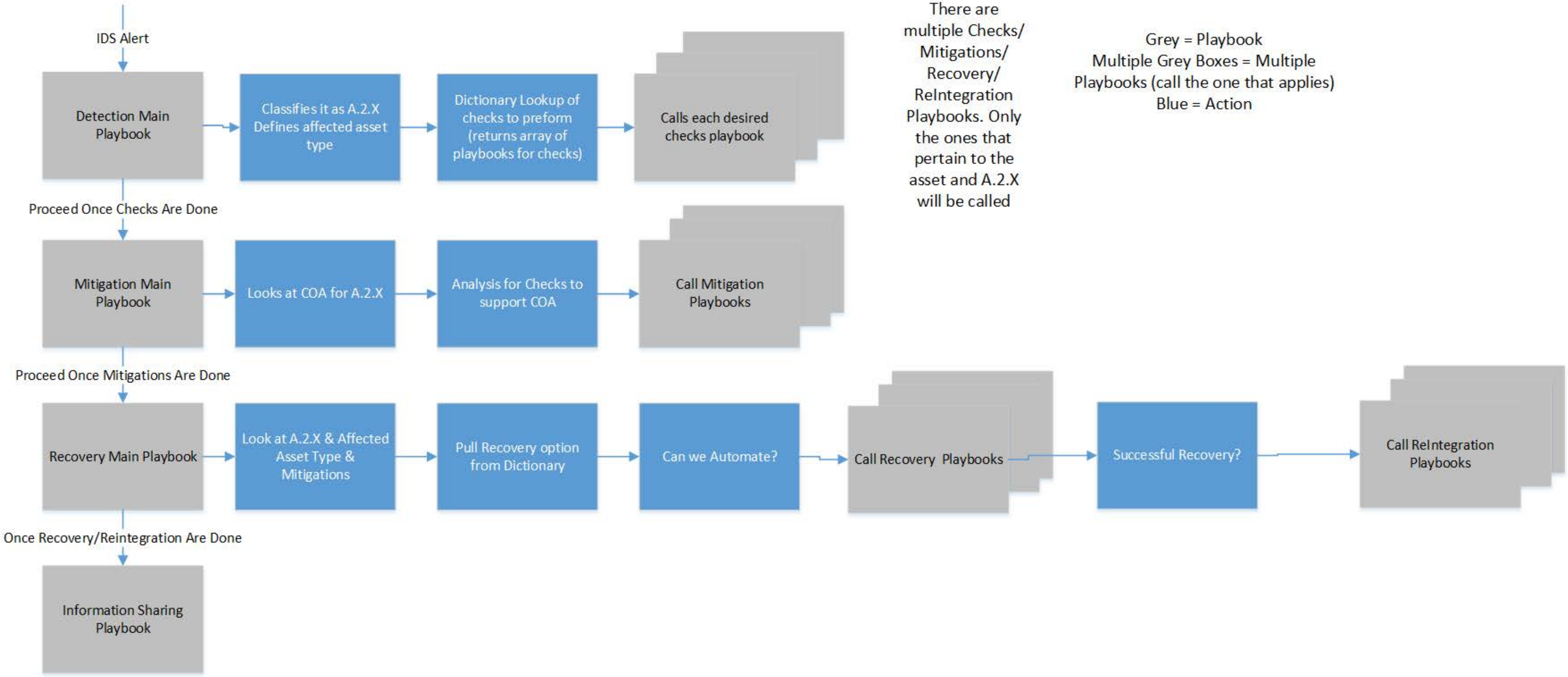


Information Sharing Playbook

Format Report

Share Report

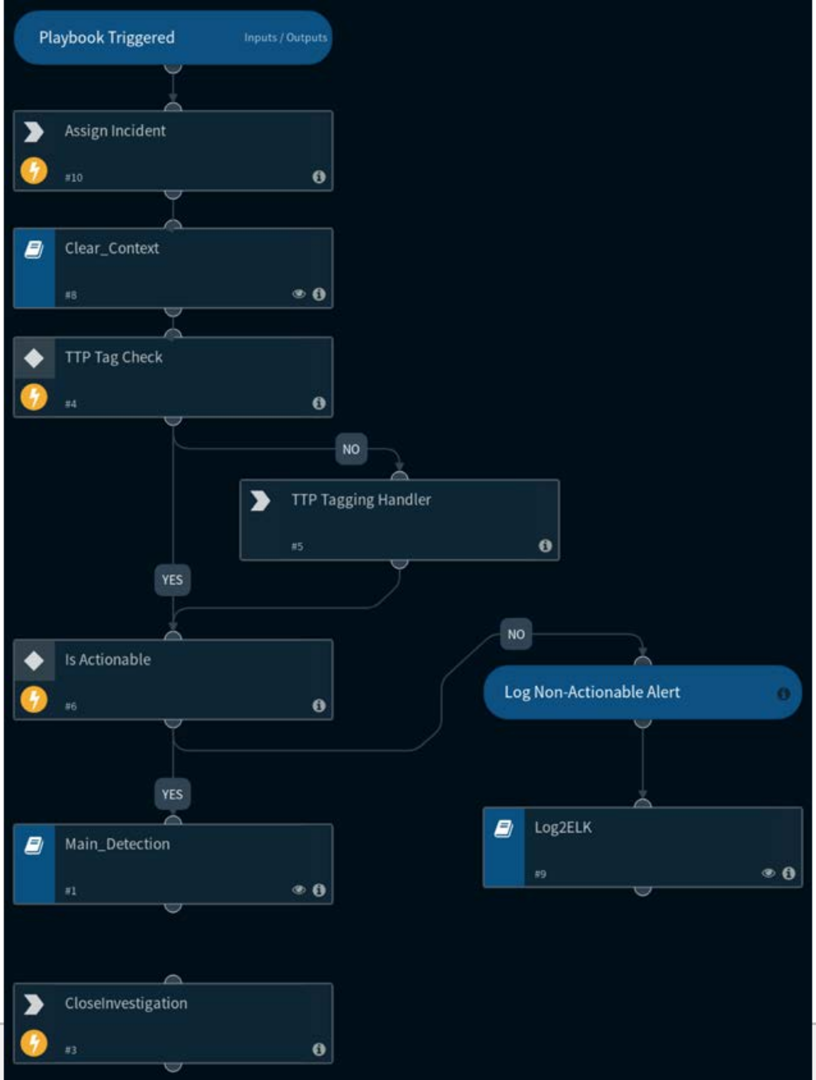
MOSAICS Playbook Details


IDS Alert
Detection Main Playbook
Classifies it as A.2.X Defines affected asset type
Dictionary Lookup of checks to preform (returns array of playbooks for checks)
Calls each desired checks playbook
Proceed Once Checks Are Done
Mitigation Main Playbook
Looks at COA for A.2.X
Analysis for Checks to support COA
Call Mitigation Playbooks
Proceed Once Mitigations Are Done
Recovery Main Playbook
Look at A.2.X & Affected Asset Type & Mitigations
Pull Recovery option from Dictionary
Can we Automate?
Call Recovery Playbooks
Successful Recovery?
Call ReIntegration Playbooks
Once Recovery/Reintegration Are Done
Information Sharing Playbook

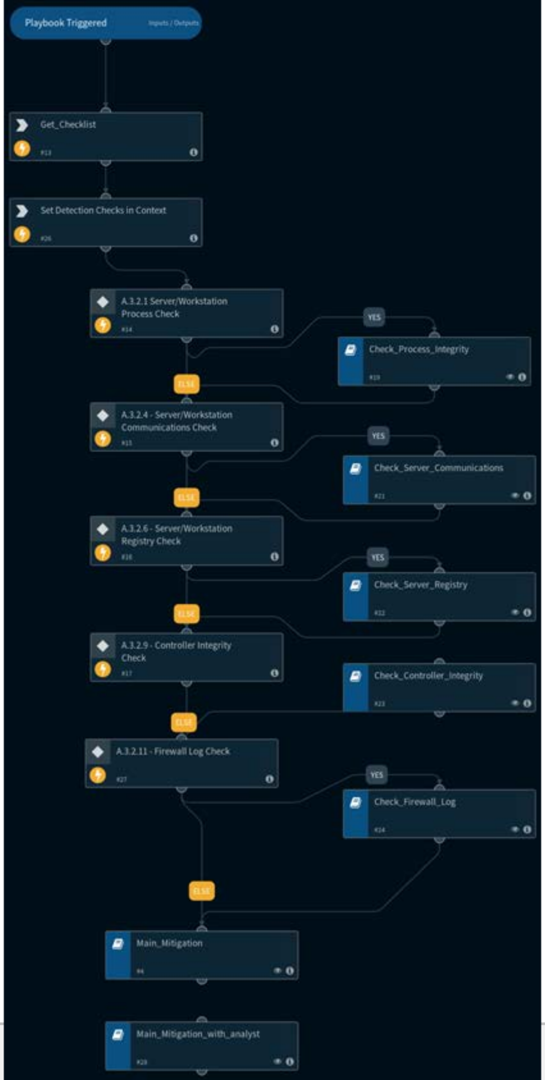
There are multiple Checks/ Mitigations/ Recovery/ ReIntegration Playbooks. Only the ones that pertain to the asset and A.2.X will be called

Grey = Playbook
Multiple Grey Boxes = Multiple Playbooks (call the one that applies)
Blue = Action

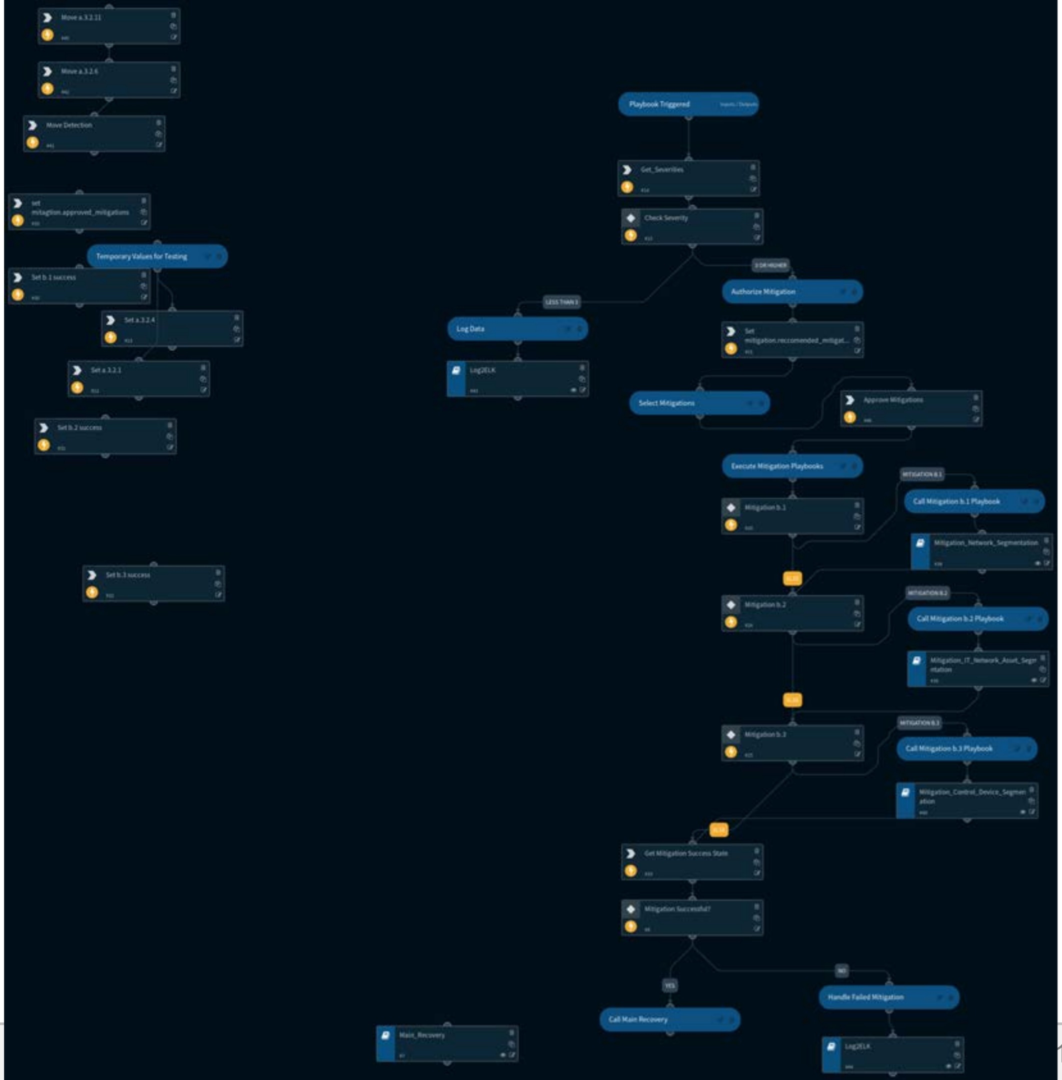
Main Ingestion Playbook



Main Detection Playbook


Playbook Triggered
Inputs / Outputs
Get_Checklist
#13
Set Detection Checks in Context
#26
A.3.2.1 Server/Workstation Process Check
#14
YES
Check_Process_Integrity
#19
ELSE
A.3.2.4 - Server/Workstation Communications Check
#15
YES
Check_Server_Communications
#21
ELSE
A.3.2.6 - Server/Workstation Registry Check
#16
YES
Check_Server_Registry
#22
ELSE
A.3.2.9 - Controller Integrity Check
#17
Check_Controller_Integrity
#23
ELSE
A.3.2.11 - Firewall Log Check
#27
YES
Check_Firewall_Log
#24
ELSE
Main_Mitigation
#4
Main_Mitigation_with_analyst
#28

Main Mitigation Playbook


Move a.3.2.11
Move a.3.2.6
Move Detection
set mitagtion.approved_mitigations
Temporary Values for Testing
Set b.1 success
Set a.3.2.4
Set a.3.2.1
Set b.2 success
Set b.3 success
Playbook Triggered
Inputs / Outputs
Get_Severities
Check Severity
3 OR HIGHER
LESS THAN 3
Log Data
Log2ELK
Authorize Mitigation
Set mitigation.reccomended_mitigat...
Select Mitigations
Approve Mitigations
Execute Mitigation Playbooks
MITIGATION B.1
Call Mitigation b.1 Playbook
Mitigation_Network_Segmentation
Mitigation b.1
ELSE
Mitigation b.2
MITIGATION B.2
Call Mitigation b.2 Playbook
Mitigation_IT_Network_Asset_Segmentation
ELSE
Mitigation b.3
MITIGATION B.3
Call Mitigation b.3 Playbook
Mitigation_Control_Device_Segmentation
ELSE
Get Mitigation Success State
Mitigation Successful?
YES
NO
Call Main Recovery
Handle Failed Mitigation
Main_Recovery
Log2ELK