OPMANTEK

NETWORK MANAGEMENT AND IT AUDIT SOFTWARE

Creating and Managing Complex Event Responses – v1 February 2019

We will send you the recording.

Submit your questions anytime. We'll do Q&A throughout.

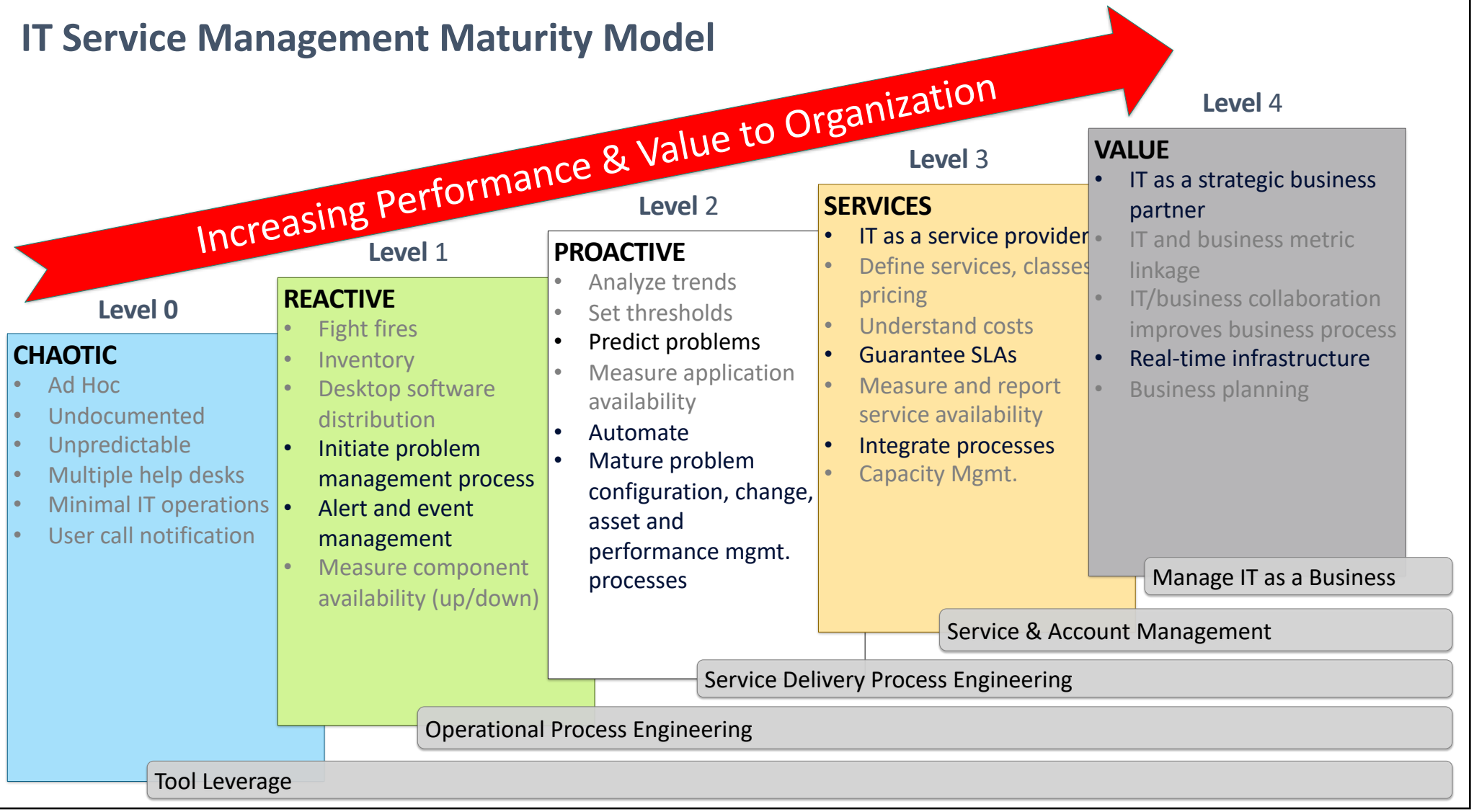
Please complete the Exit survey.

Topics for Today

In today's session we will explore the concept of using opEvent's Actions to create a Complex Adaptive System (CAS) to handle troubleshooting and event remediation. In this 60-minute session we will cover –

- Core concepts of a CAS system and how implementing it will improve maintainability and scalability of the solution
- Methods for designing the overall event escalation system
- How to create useful troubleshooting scripts, including collecting device configuration information, for every event
- Building notification routines to handle all situations; after hours, weekends, vacations, and non-response
- Expanding actions to proactively respond to events; reconfiguring devices (using opConfig), restarting services, and leveraging APIs

IT Service Management Maturity Model



Architecting a Solution

Open-Source

NMIS – Fault and Performance Monitoring

Commercial Solutions

opEvents – Advanced Event Management and Response

opConfig – Capture, track and push configuration changes

Useful References

Where can I go when I have questions?

- NMIS Wiki – https://community.opmantek.com/display/NMIS/Home
  - Plugins - /usr/local/nmis8/conf/plugins/README
- opEvents Wiki – https://community.opmantek.com/display/opEvents/Home
  - Setup Email Notifications and Other Actions - https://community.opmantek.com/x/oYh4AQ
  - Actions and Escalation - https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation
- opConfig Wiki – https://community.opmantek.com/display/opconfig/Home
  - Automating Configuration Changes - https://community.opmantek.com/x/JQH6
  - Plugins- https://community.opmantek.com/display/opconfig/Plugins+in+opConfig
- Community Questions Board - https://community.opmantek.com/questions
- Support Issues – support@opmantek.com
- Sales – usa@opmantek.com

Past Webinars

You should view these webinars and become familiar with their concepts first

- https://opmantek.com/webinar-advanced-diagnostics-and-network-automation-with-opevents/

  https://opmantek.com/webinar-collecting-non-ssh-telnet-device-configurations/
- https://opmantek.com/responding-to-unauthorized-configuration-changes-using-opconfig-and-opevents/
- https://opmantek.com/webinar-expanding-on-snmp-wmi-collection-with-nmis-collect-plugins/

Example Event Response

- First touch could be 30-60m, depending on workload and available technicians
- Set priority by # affected customers, customer VIP status, time of day
- Send outage email (dependent on day of week, time of day)
- Create helpdesk ticket, assign to NOC technician
- Ping device; acceptable latency?
- MTR; change in routing?
- Collect device configurations, compare to previous configuration
- If event is service related, restart the service
- If event does not clear after service restart, restart device
- Update website for outage area, affected users
- Dispatch field services (via email)

Introduction

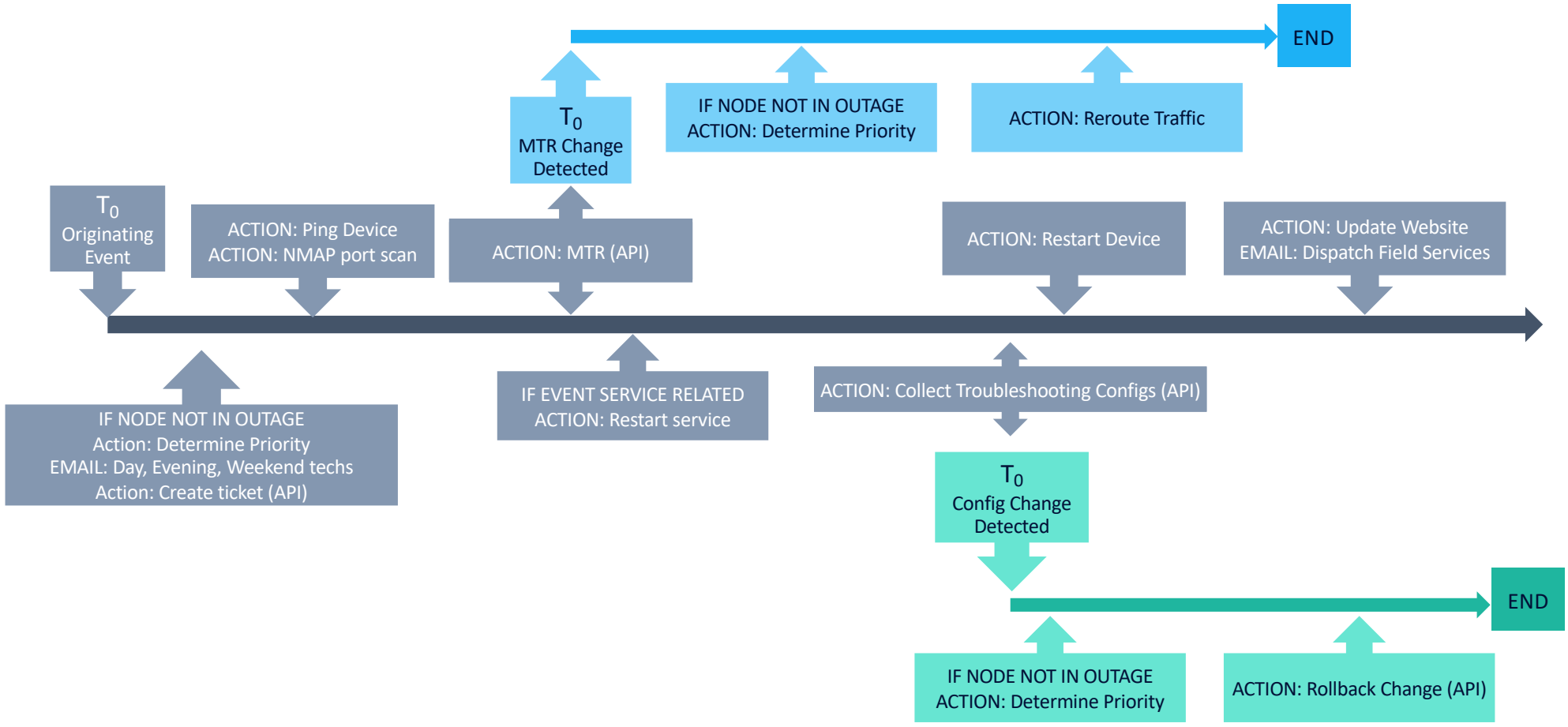
What Is, and Isn't a Complex Adaptive System (CAS)

Complex Adaptive Systems (CAS) are systems that have many components, or agents, that interact and adapt, or learn.

- Many agents that interact dynamically, but may be ignorant of the system as a whole
- Interactions are rich, and may affect or be affected by other agents in the system
- Interactions are non-linear, and can feed back on themselves
- Overall behavior is not predicted by the behavior of the individual agents
- Complex systems have a history, they evolve, and their past is co-responsible for the present behavior

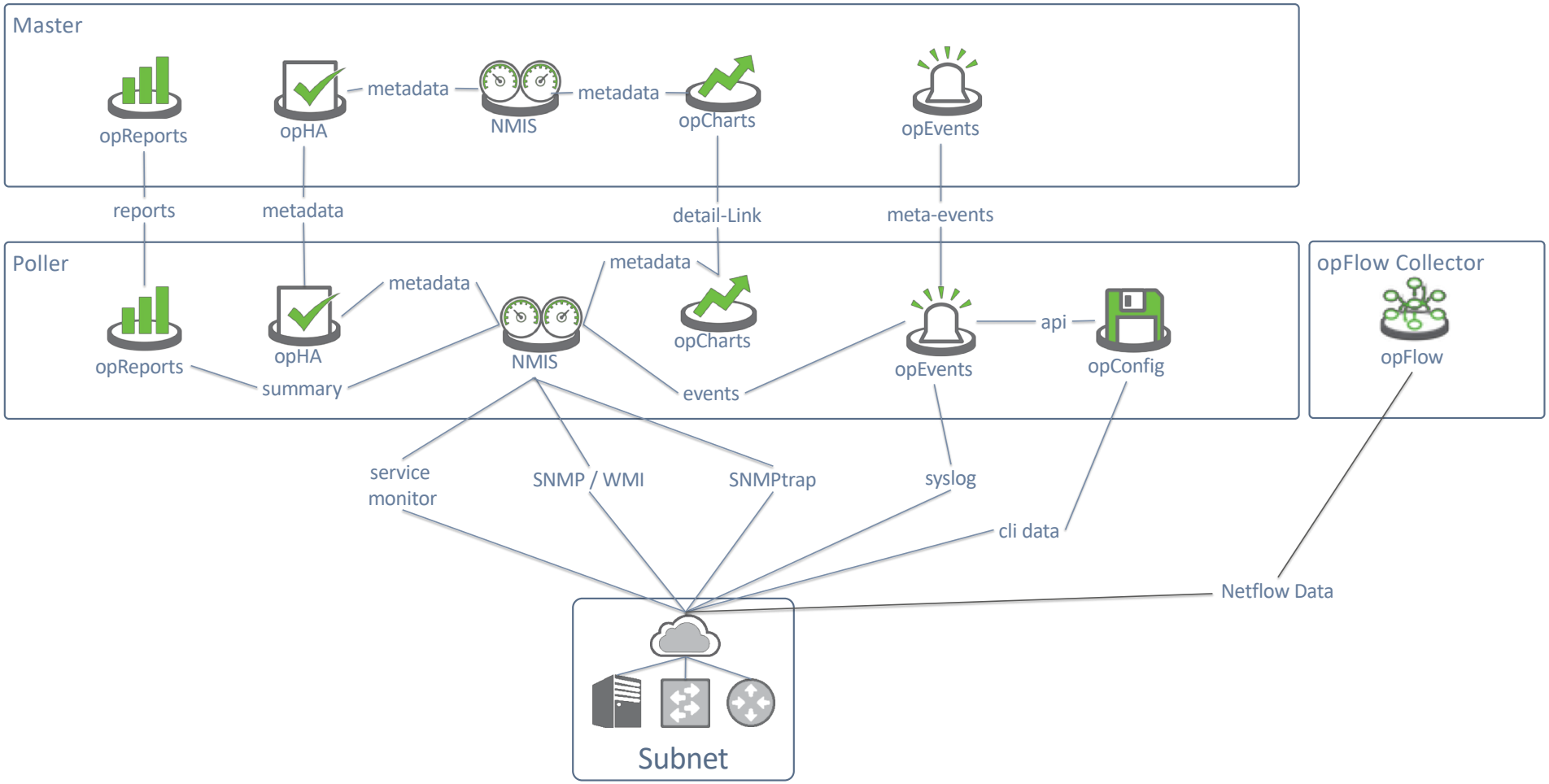
Example Event Response

Rethinking the Example Event into a CAS using opEvents and opConfig



Event Automation Using opEvents

Opmantek Application Flow



opEvents

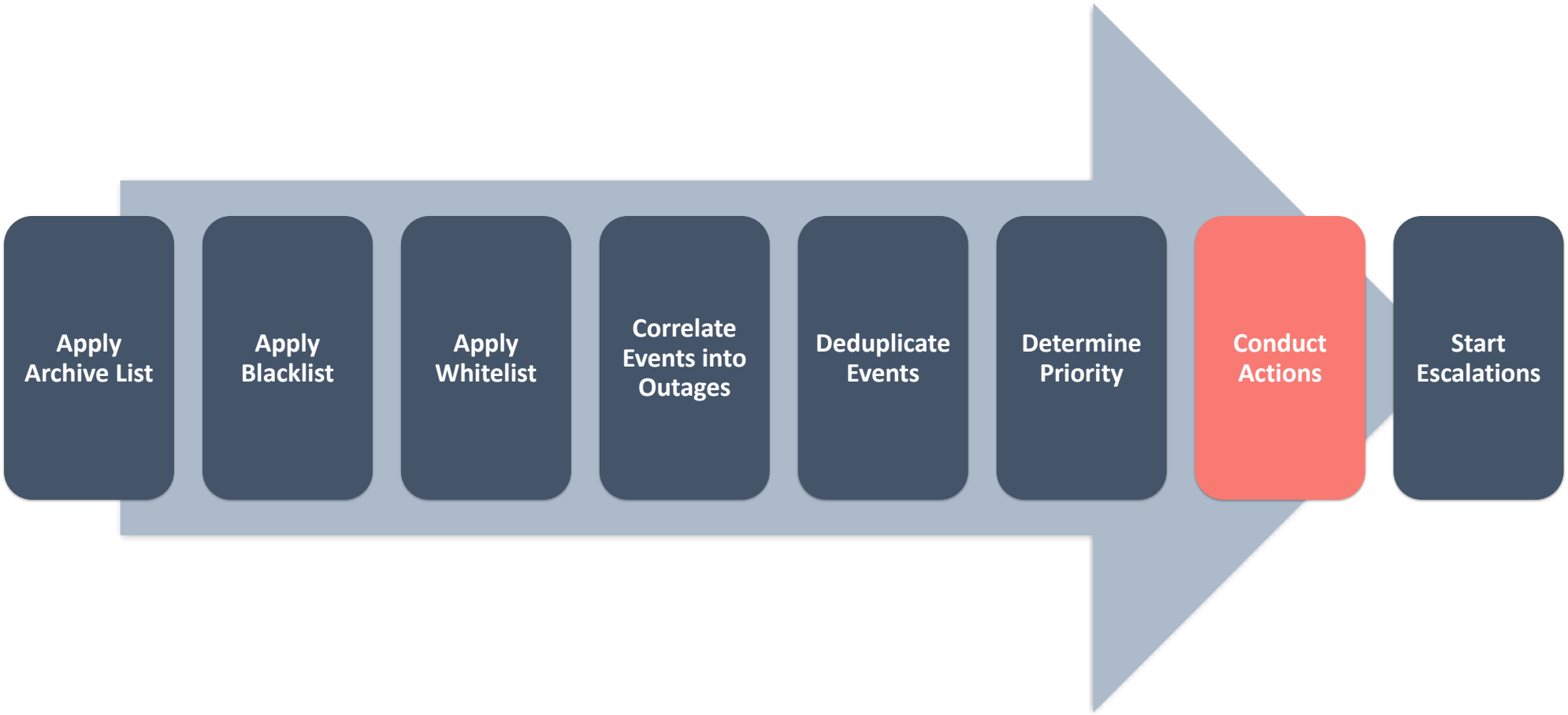
Advanced Fault Management and Operational Automation

WHY – Expands on efforts already done through NMIS, and scientifically improves automated response thereby decreasing workload and improving operational efficiency

- Enhances and builds-on NMIS' Thresholding, Escalation and Notification systems
- Support whitelisting and blacklisting of events
- Handles event correlation, deduplification, event storms, and event flap
- Allows application of event Actions, or responses to events
- Supports flexible escalation and notification
- Supports custom email templates per contact

Event Processing Flow

These are all background processes…



Basic Event Automation

Using opEvents' Actions to Automate Everyday Troubleshooting and Repair

Four Clear Steps to Event Automation

1. Identify the top network events you respond to frequently (daily, weekly, etc.)
2. List the steps you take – troubleshooting and remediative - when the issue occurs
3. Identify how these steps can be automated
4. Create an Action to respond to the event

Developing a Complex Adaptive System

CAS

Understanding the Building Blocks for Creating CAS Agents/Components

- opEvents Correlations – to create new synthetic events from base events
- opEvents Policy – if/then rules to fire off scripts and escalations
- opEvents Escalations – to create new paths for activities
- opEvents Scripts – execute complex bits of log and return the results back to opEvents
- opEvents API - to raise new events based on the output of comparison/calculations
- opConfig Commands – execute command(s) against a given device via CLI, can be expanded with opConfig plugins, gives access to device credentials, can raise events
- opConfig Configuration Push – change a device's configuration via the CLI
- NMIS Collect and Update plugins to change collection behavior
- opTrends to replace NMIS static Thresholds

opEvents Event Actions

Event Correlation

Defined In: /usr/local/omk/conf/EventRules.nmis

Ex: 3+ Device Reset events at the same Location within 3m becomes a Location Power Outage

Use Event Correlation when the response taken to the synthetic event would be different from that taken for the individual event(s) that comprise it

- Once event Correlation occurs child event processing is suppressed

https://community.opmantek.com/display/opEvents/Event+Correlation

Event Policy

Defined In: /usr/local/omk/conf/EventActions.nmis

```
'110' => {
        IF => 'event.stateful =~ qr{BGP Peer}',
        THEN => 'priority(8) AND script.ping_node() AND script.ping_neighbor() AND script.troubleshoot_bgp()',
        BREAK => 'false'
},
```

Use Policy Rules to start the event management process

- Policies are called just once for each event
- Simple If/then statements can be nested, and are executed from top to bottom

https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation

Event Escalation

Defined In: /usr/local/omk/conf/EventActions.nmis

Use Escalations to create time-controlled responses

- Escalations can be called from any section, i.e. Policy, Script as escalate.*policyname()*
- Escalations can call any Action; i.e Script, Log, Email
    - Exception - an Escalation policy cannot call another escalate.*policyname()*
- Escalations run while the event driving the policy rule is in effect

https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation

Event Scripts

Defined In: /usr/local/omk/conf/EventActions.nmis

Use scripts to conduct complex actions, collect troubleshooting information, execute external scripts

- Scripts can be called from any section, i.e. Policy, Escalate as script.*scriptname()*
- Scripts can do anything, from troubleshooting to remediative in nature

https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation

Event API

Create New Events or Retrieve Event Details

Use the opEvents API to create new synthetic events with their own Policy Actions and Response

- The new event is generated directly into opEvents and is not processed through NMIS
- New event is NOT dependent on status of the original event that created it

https://community.opmantek.com/display/opEvents/opEvents+REST+API+Reference

opConfig Plugins and Configuration Push

opConfig Plugins Development Patterns

When and Why You Might use opConfig Plugins

- Collecting arbitrary data NOT from SSH/Telnet CLI and storing it
- Looking up and beautifying data
- Running multiple commands and comparing the output to create a result
- Doing weird stuff (technical term) which is only resolved by writing code

https://community.opmantek.com/display/opconfig/Plugins+in+opConfig

opConfig Plugins

Expanding on opConfig's Command Collection System

- Augment and extend the Command Collection functionality
- Two classes
  - Collecting device configurations
  - Processing to filter or transform configuration data collection
- Stored in: /usr/local/omk/conf/config_plugins/

Pushing Configuration Changes

Leveraging opConfig's Push Capability via opEvents' Actions

Example EventActions Policy

```
'40' => {
        IF => 'node.roleType eq "core" and node.type eq "router" and event.event eq "Node Configuration Change"',
        THEN => 'script.reset_routerconfig()',
        BREAK => 'false'
},
```

Example EventActions Script

```
'reset_routerconfig' => {
        arguments => 'act=push_configset name=routerconfig at=now+1minute nodes=event.node',
        exec => '/usr/local/omk/bin/opconfig-cli.exe',
        output => 'save'
},
```

```
opconfig-cli.pl act=push_configset name='set name' [info=0/1][node=nodeX][nodes=nodeA,nodeB...][at='time spec']
```

https://community.opmantek.com/display/opconfig/Automating+Configuration+Changes+with+opConfig

NMIS Plugins

NMIS Plugins Development Patterns

When and Why You Might use NMIS Plugins

- Cross linking data in NMIS
- Looking up and beautifying data
- Collecting arbitrary data NOT from SNMP and storing it
- Doing complex SNMP queries, mainly where the indexes are unused or derived
- Doing weird stuff (technical term) which is only resolved by writing code

NMIS Plugins

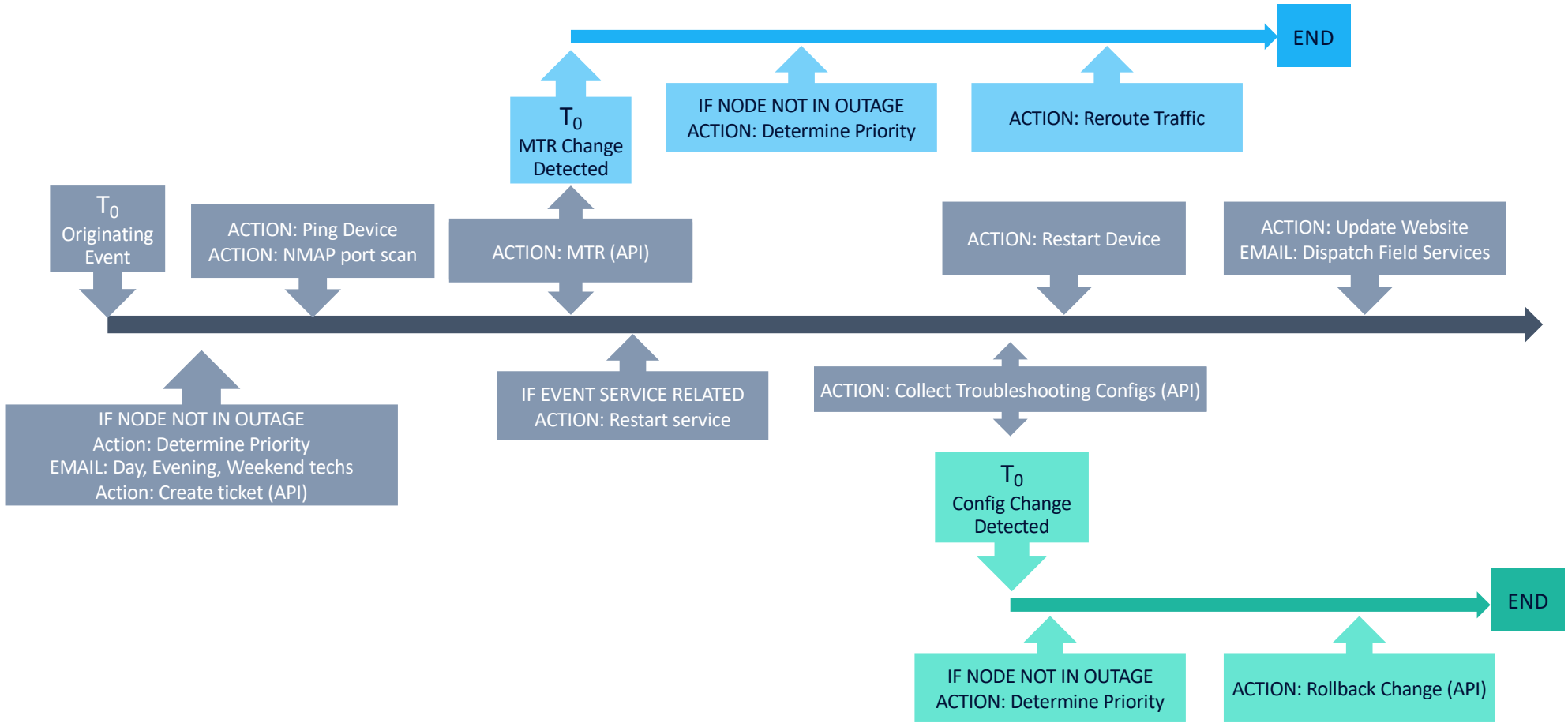
Expanding on NMIS' Modeling System

- Augment and extend the Update and Collect functionality
  - NMIS Update cycle runs 1x/day to gather static, non-performance data
  - Collect scheduler runs 1x/minute, uses assigned Polling Policy for frequency
- Four classes
  - collect_plugin and update_plugin – runs for each node
  - after_collect_plugin and after_update_plugin – runs once at end of operation
- Stored in: /usr/local/nmis8/conf/plugins

Developing a Complex Adaptive System

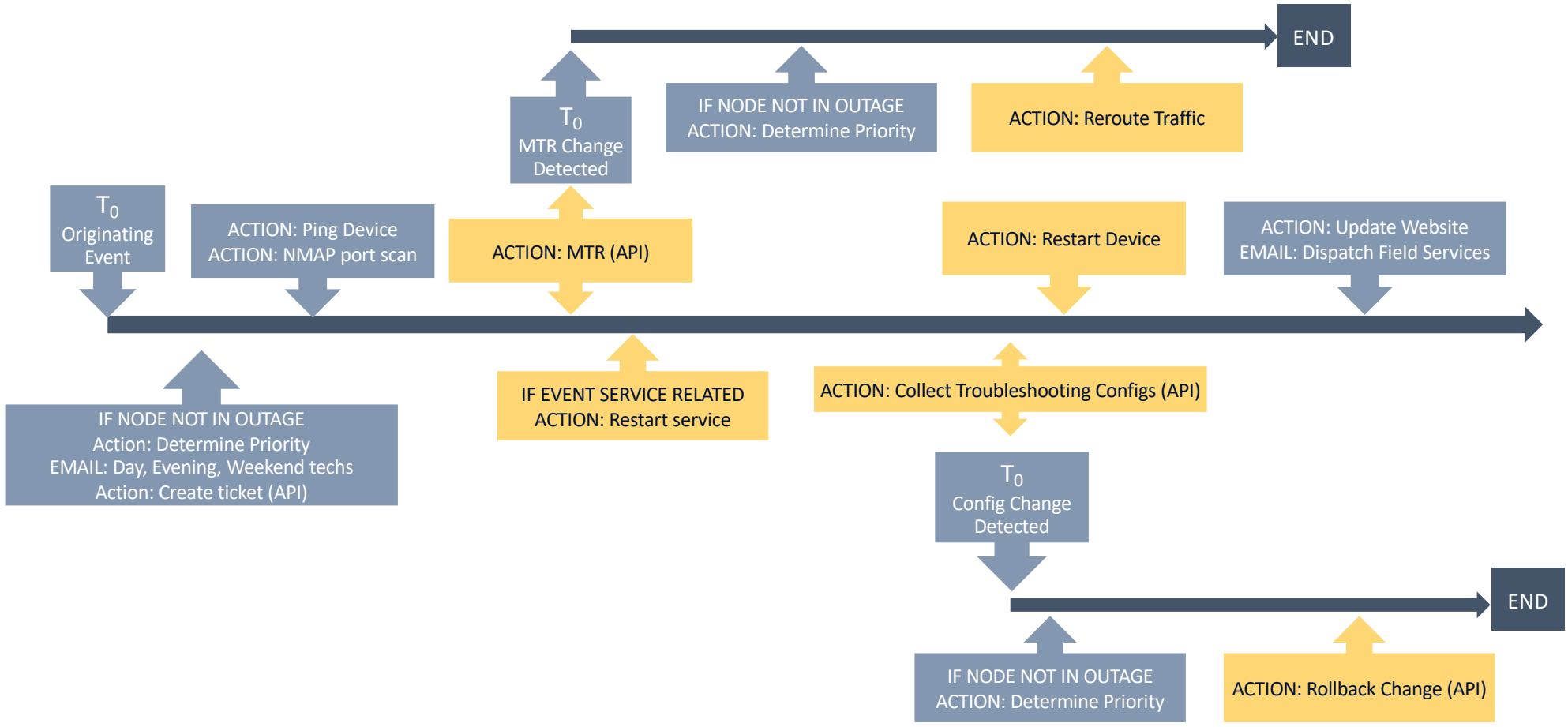
Example Event Response

Rethinking the Example Event into a CAS using opEvents and opConfig



Example Event

Blocks in Yellow are Fulfilled by opConfig



Building a CAS

A Process for Developing a CAS Solution

1. Identify an individual event
2. List the steps you take – troubleshooting and remediative - when the issue occurs
3. What automated action(s) can, and should be carried out (data collection, remediation)
4. Identify WHO needs to be contacted, and WHEN (working hours, after hours, weekends)
5. What should happen over time if event is NOT acknowledged (remains active)

CONTACT FOR FOLLOW UP

Commercial enquiries:

Tom Wiri
Account Executive
+1 (512) 430-4450
usa@opmantek.com

Technical enquiries:

Mark Henry
Senior Engineer
+1 (207) 951-2428
markh@opmantek.com

OPMANTEK