Ondaro

Event Management & AIOps

CMDB MasterClass Part 8

Chris Padmore & Christine Morris

June 11, 2025

Agenda

Welcome & Introduction

1. IT Operations
2. Event Management Overview
3. AIOps Overview
4. Event + AIOps
5. Best Practices
6. Q&A

At Ondaro, we help organizations turn complexity into clarity — and make ServiceNow a catalyst for what's next.

You're not just implementing software.
You're simplifying systems, empowering teams, and delivering meaningful impact.

Whether you're starting small or scaling enterprise-wide, Ondaro is here to help you navigate the wave of what's next — and make transformation real.

Where Deep Expertise Meets Consistent Results.

Driving real change takes both platform knowledge and a partner who is with you every step of the way.

8,500+

Certifications & Accreditations

13 | 7

Product Line Achievements and Validated Practices

3 years

Average length of client partnership

4.69 / 5

Customer Satisfaction score

Ondaro is the only pure play ServiceNow partner with fully certified resources across the platform

ITSM

ITOM

ITAM

HRSD

CRM

SPM

SECOPS

IRM

APP ENGINE

ENVISION

Business Transformation

Organizational Change Management

AI-Readiness

Platform Strategy & Governance

IMPLEMENT & DEVELOP

Platform Architecture & Engineering

Product Implementation

UX & UI Design

App Development

Data Management & Integrations

MANAGE & OPTIMIZE

Platform Operations

Enhancement Services

Product Management

Join the Conversation: Using Teams

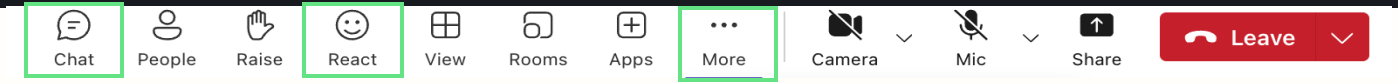
Turn on Video
Let's get interactive and enjoy ourselves!

Unmute – Click the microphone icon to unmute and participate

Chat – Message everyone or just one person

Get Help – Use Chat

Show Captions - Click More, Language & speech, Show live captions

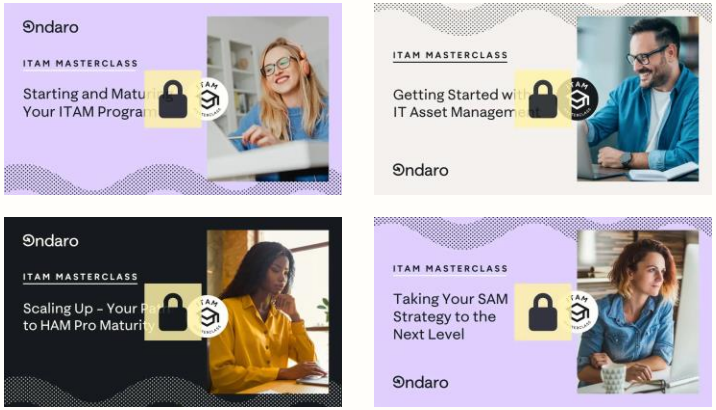


Catch up with our

CMDB & ITAM MasterClass Series!

CMDB MASTERCLASS

Join for our 9th CMDB MasterClass on CMDB + Vulnerability Management July 30th!



ITAM MASTERCLASS

Find recordings, resources & more!

Ondaro

Welcome to IT Operations

Welcome to IT Operations

- Multiple Tools
- Siloed Teams
- Swivel Chair
- Multiple Platforms
- Disconnected Processes
- Legacy Systems
- Unexplained Outages

Ondaro

Event Management Overview

> Monitor the health of services and infrastructure using a single management console and respond appropriately to any issues that come up. Event Management provides intelligent event and alert analysis to ensure continuity of your services' performance.

Lorem ipsum dolor

What is Event Management

Event Management helps you to identify health issues across the datacenter on a single management console. It provides alert aggregation and root cause analysis (RCA) for discovered services, application services, and automated alert groups.

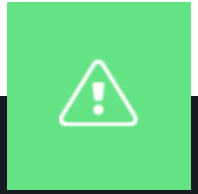
Goals of Event Management

- **Ingest** events from 3rd party monitoring and Agent Client Collector
- **Correlate** events with event rules to reduce noise from multiple systems
- **Map to CIs** to simplify the task of remediation
- **Create Tasks** to provide remediation efforts and reduce MTTR
- **Remediate** on alert with automated remediation steps

Event Management - Use Cases

Collect events from multiple monitoring sources

Correlate multiple events to reduce ticket volumes



Maps events to CIs, perform service impact analysis and create an incident task from the alert

Difference Between Events, Alerts, and Incidents

Events

A notification from one or more monitoring tools that indicates something of interest has occurred such as a warning or failure

Example: Disk space available is less than 10%

Alerts

Alerts are created when conditions or rules are met that require someone to take action on an event.

Example: If disk space available is less than 10% on an assembly line controller, then create a Critical Severity Incident and assign it to the proper group to take action.

Incident

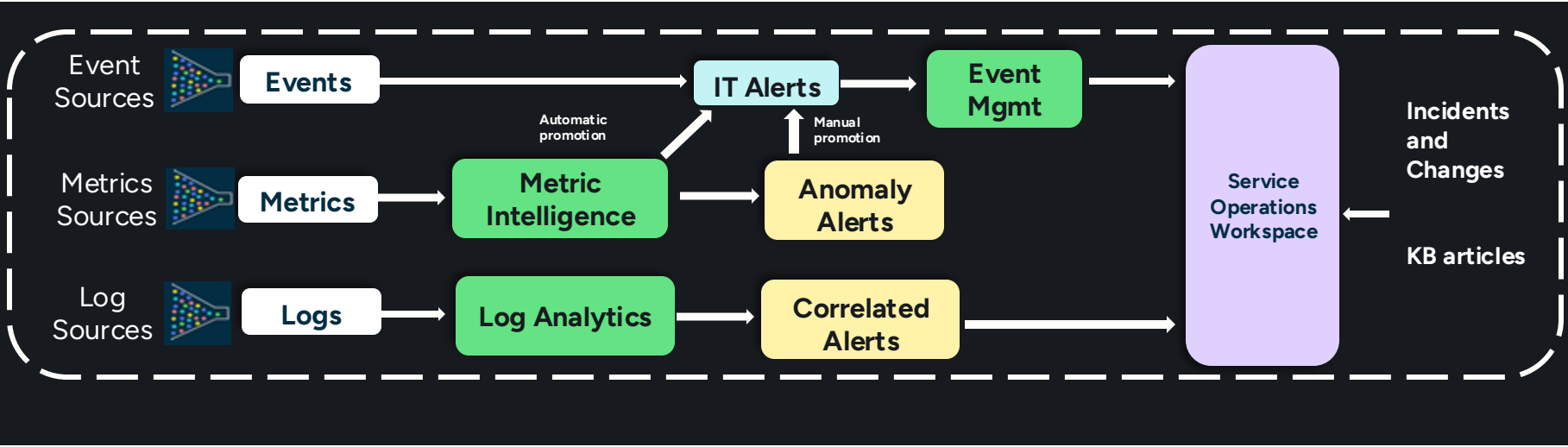
Incidents are derived from one or more unplanned events that negatively affect business services and require remediation

ITOM Health for events, metrics and logs

Event Management receives and processes events from external monitoring tools or from Agent Client Collector for Monitoring. Events are converted into alerts internally. Note: An alert in a monitoring tool (such as SolarWinds) is still considered an event in ServiceNow ITOM

Metric Intelligence processes metrics from external sources (metric connectors) or from Agent Client Collector for Monitoring

Log Analytics processes logs from external sources (via connectors). Will create IT alerts based on its own correlation



Event Management Process

Events & metrics

Which events are of interest?	What is the root cause?	Which services are impacted?	What else should I know?
Event & Metrics Processing	**Alert Correlation & RCA**	**Service Impact**	**Related Intelligence**
			
• Normalize • De-duplication • Filtering • Transformation • Bind to CIs • Metrics in time-series DB	• Human-based correlation rules • ML-based grouping • CMDB-based grouping • Anomaly detection • Topology-based root cause analysis (RCA)	• Services impacted by alerts • Service maps	• Similar alerts on related CIs • Related knowledge articles (NLP) • Related ITSM Incidents, Problems, Changes

Major Actors for Event Management

Event Admin

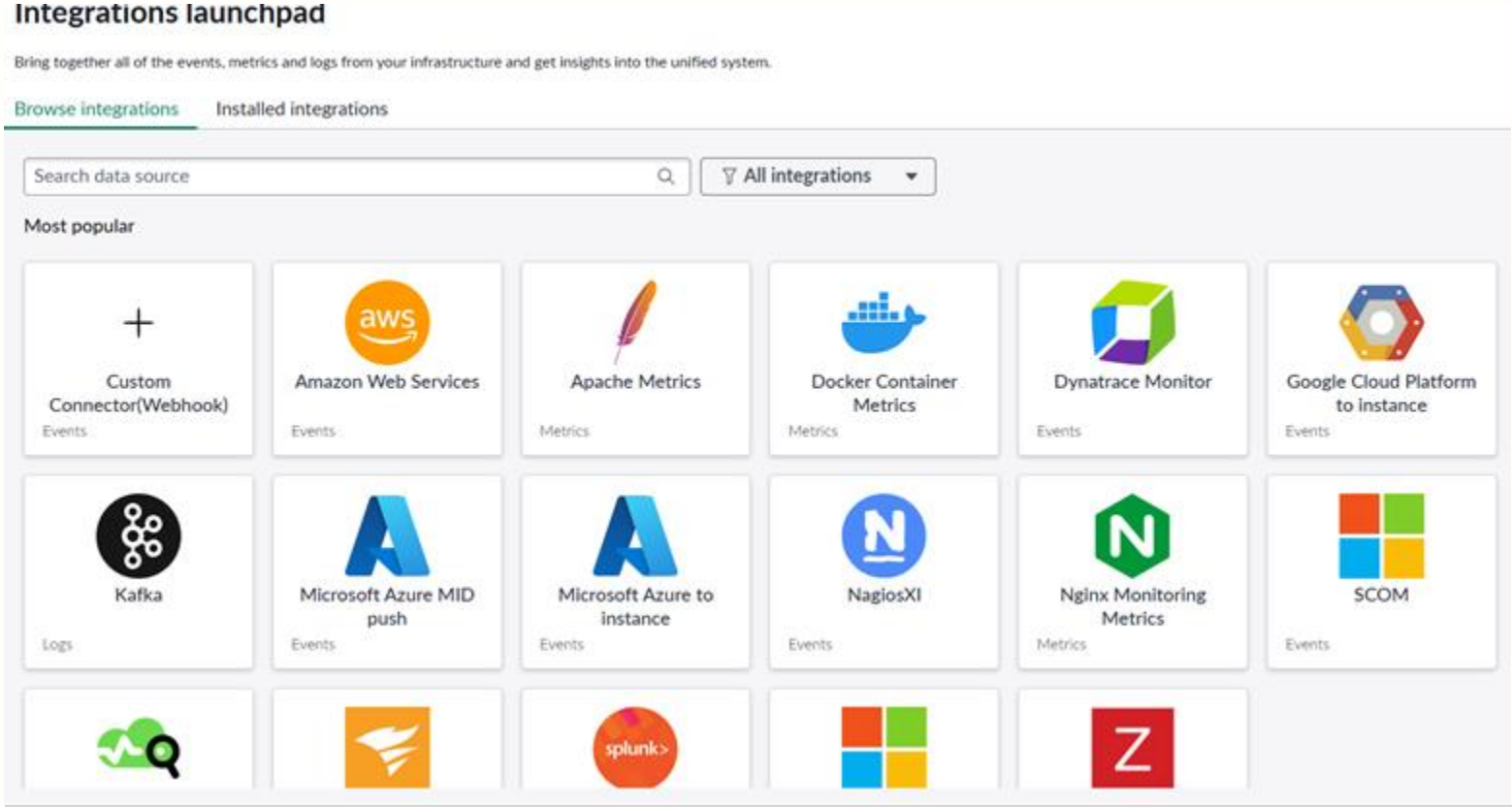
- Ingest event data
- Review the Integration Health state
- Suppress noise by creating an Ignore automation
- Enrich the ingested data with additional context and information
- Group alerts based on the extracted and out of the box shipped tags
- Create response automation

Event Operator

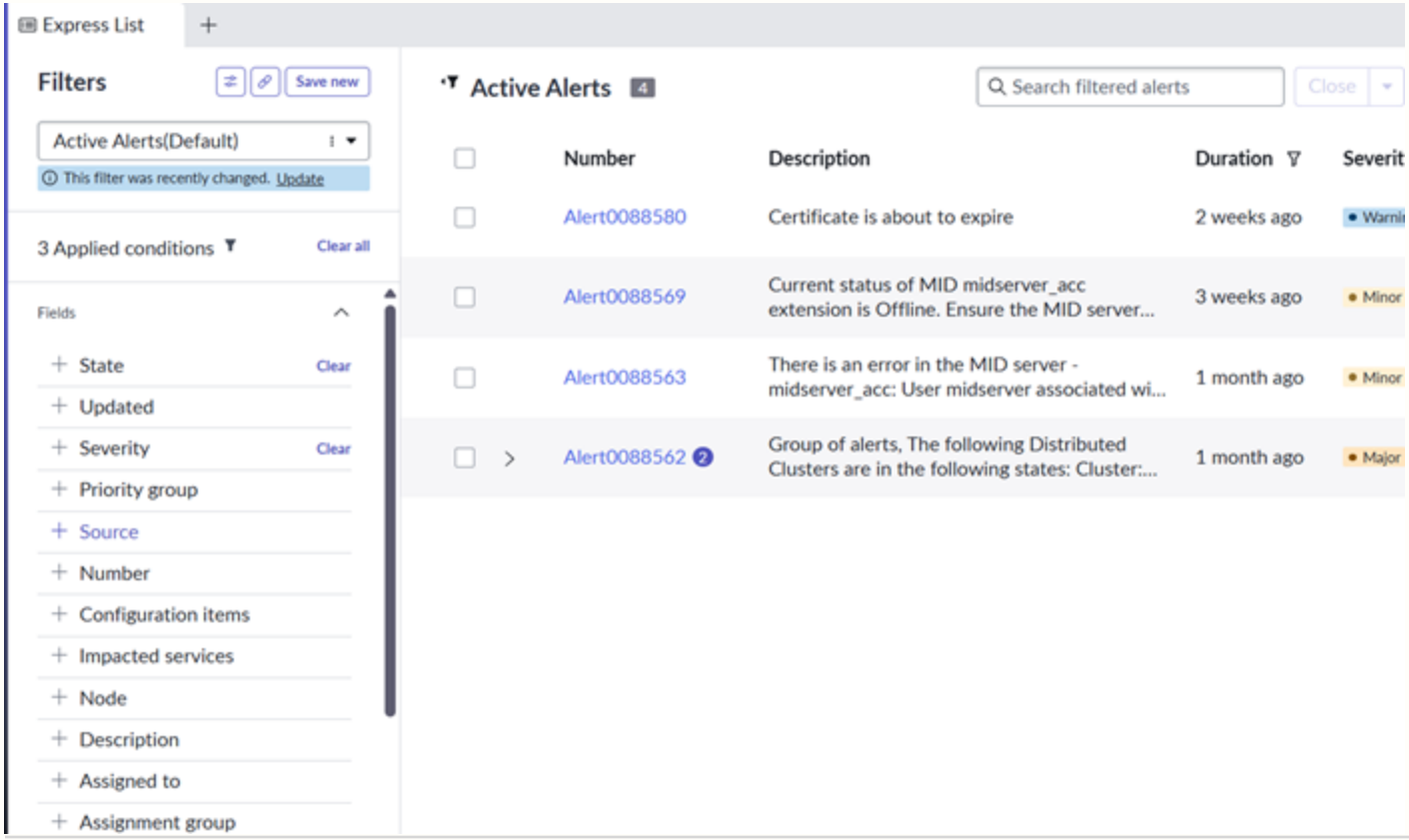
Investigate and Triage alerts

- By using Gen AI Alert Analysis
- Reviewing the link-view
- Exploring the timeline

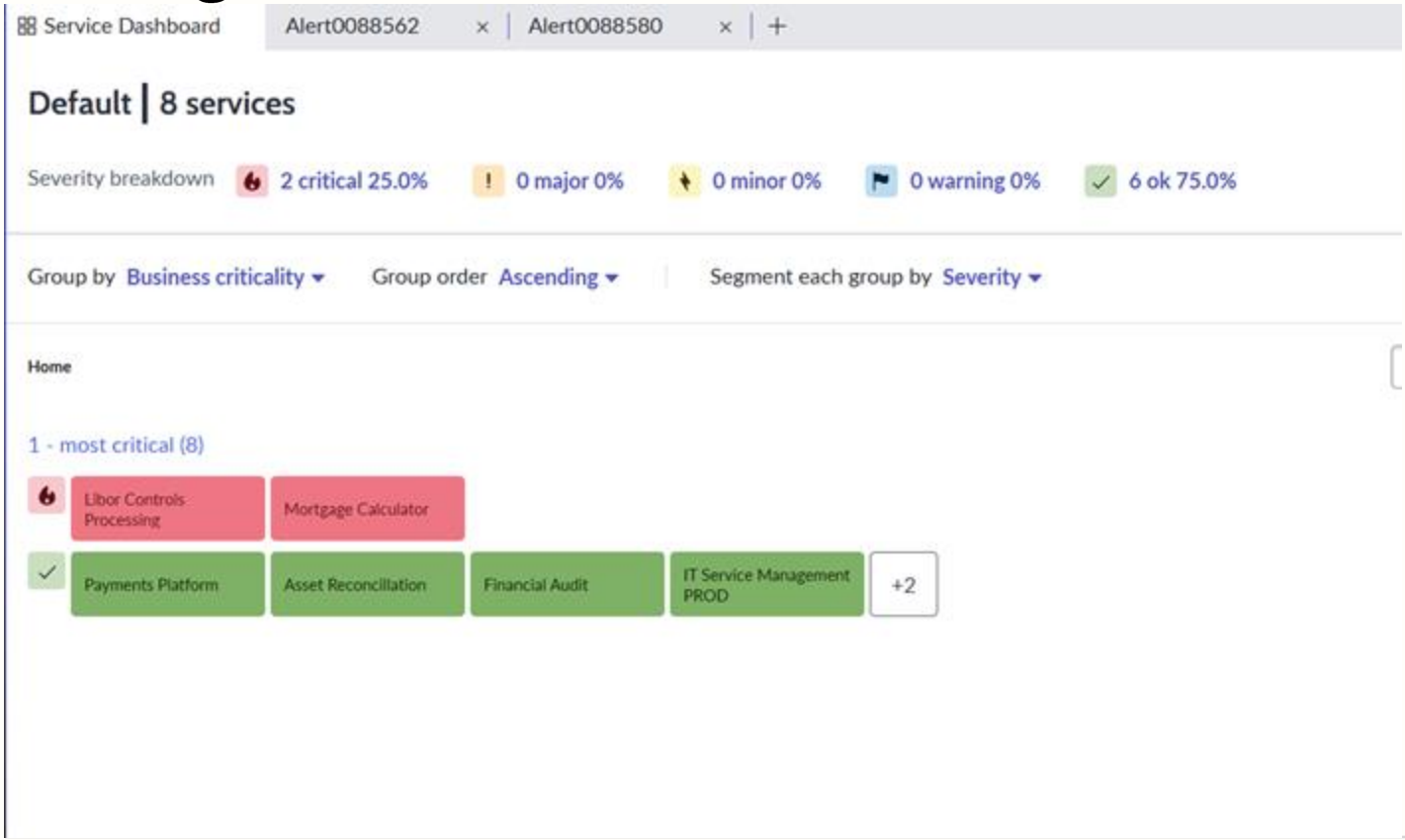
Ingest Data Faster



Review Data Faster



Manage Services Easier



AUDIENCE POLL

How are you monitoring your environment today?

A. We use various monitoring solutions

B. We mainly use log analytics, like Splunk

C. We mainly rely on one monitoring tool

D. People email us with problems

Ondaro

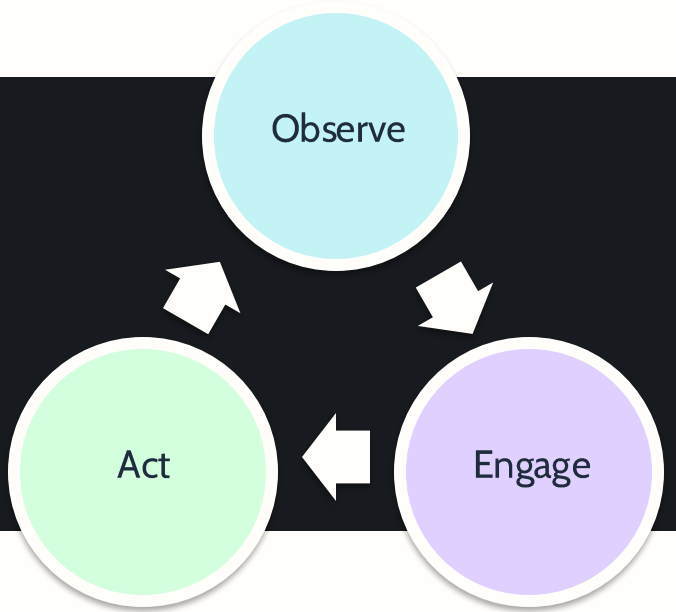
AIOps Overview

AIOPs Approach

Artificial Intelligence for IT Operations

WHAT IS ARTIFICIAL INTELLIGENCE?

"The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."



Main Features of Predictive AIOps

Anomaly Detections

Detects unusual patterns or deviations from normal operating parameters across IT infrastructure and system to provide early detection to IT Teams

ML Feedback

Control the threshold of normal behavior by providing ML Feedback to alerts

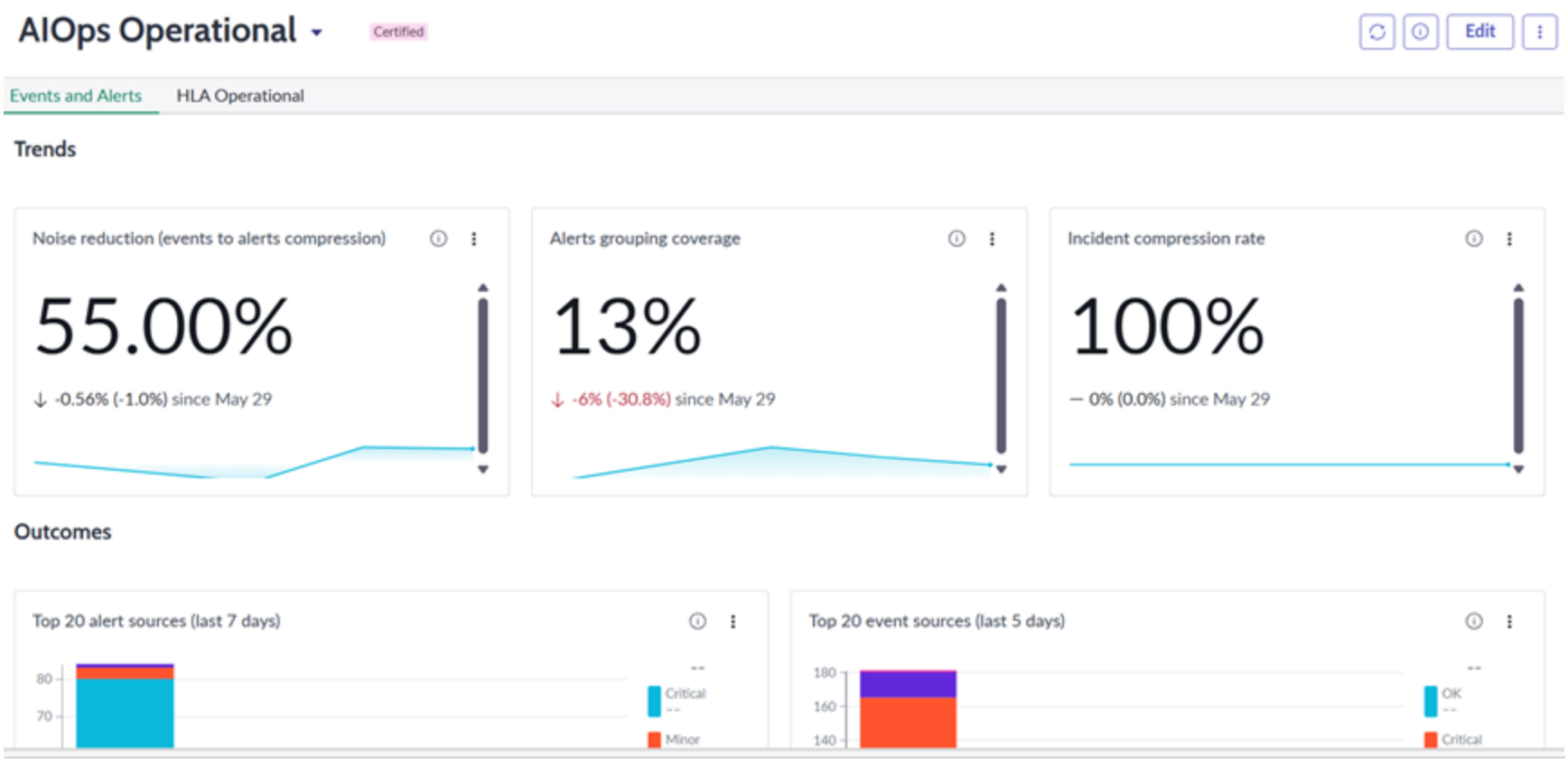
Automated Root Cause Analysis

Get suggested root cause and remediation steps generated by Now Assist to reduce research time into remediation

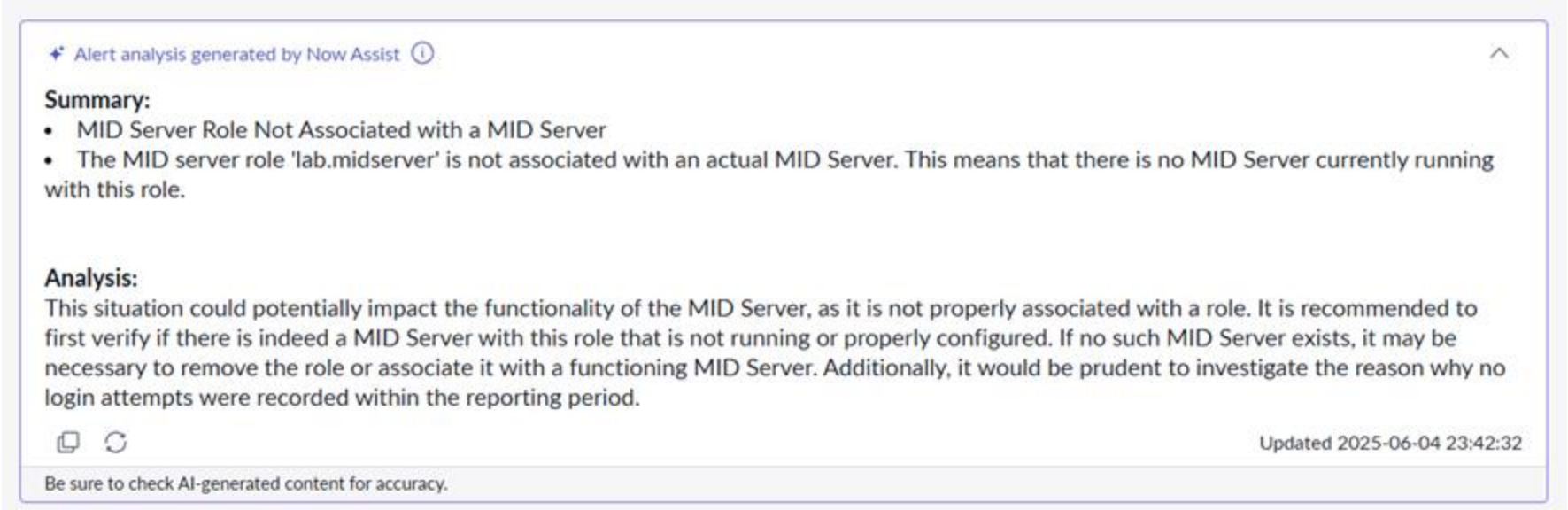
Remediation Playbooks

Standardize procedures for resolution by leveraging remediation playbooks to direct teams to perform corrective actions or kick-of automated self-healing

AIOps Workspace



Now Assist for ITOM



AUDIENCE POLL

Who manages your alerts today?

A. Each monitoring team handles their own alerts

B. Each application team handles their own alerts

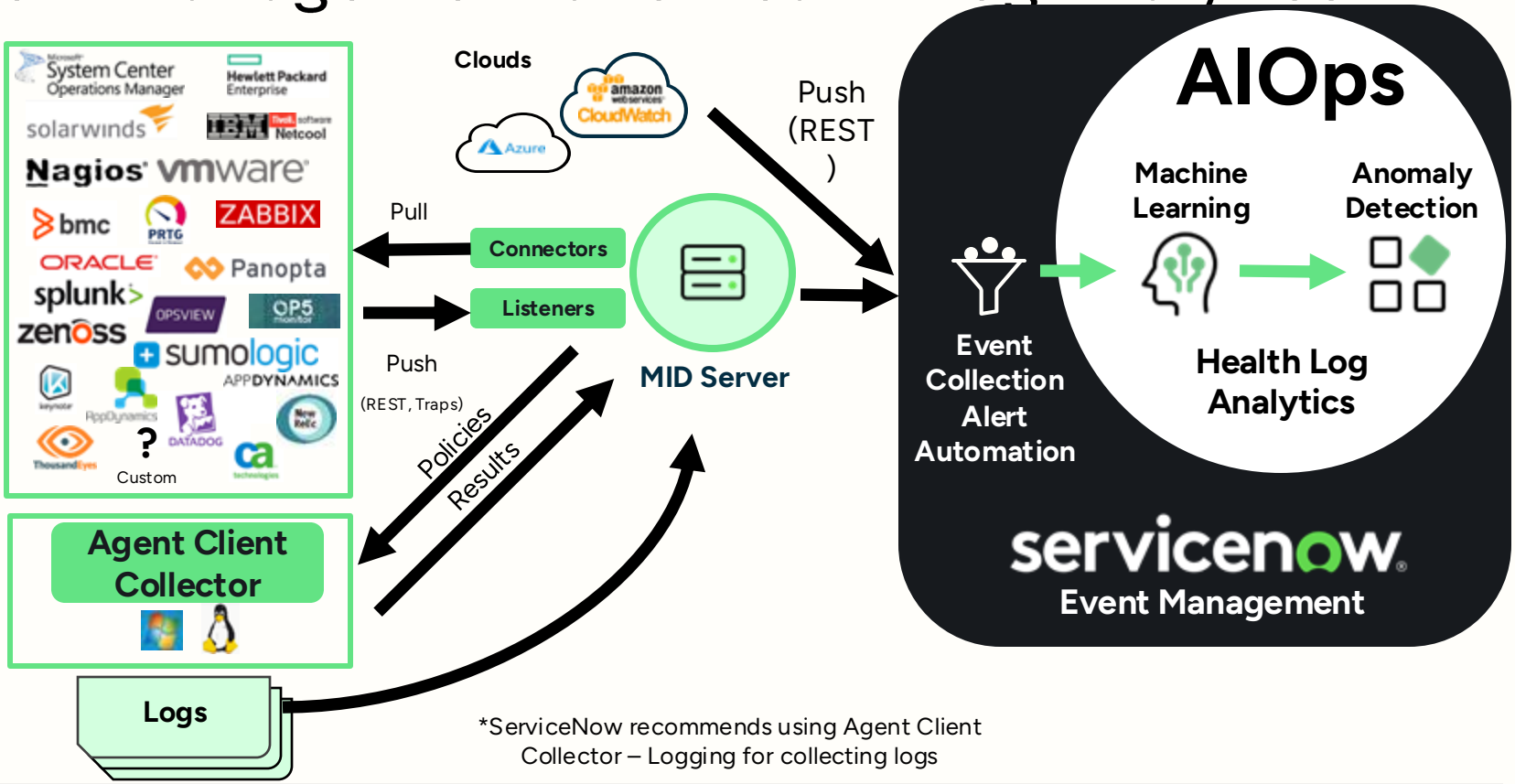
C. We have a centralized response team that handles all alerts

D. We've never resolved an alert

Ondaro

Putting it all together
Event Management & AIOps

Event Management and Health Log Analytics



*ServiceNow recommends using Agent Client Collector – Logging for collecting logs

ITOM AIOps Agents persona

Sam Robinson

AIOps Specialist, Retails.com

Problem

Reactive Operations

Operators are stuck in a reactive state, triaging and resolving alerts while mainly dealing with repetitive tasks and having limited access to third-party observability tools.

This reactive approach impacts business continuity and customer satisfaction, and high operations costs.

Solution

Transition to AI Supervisor

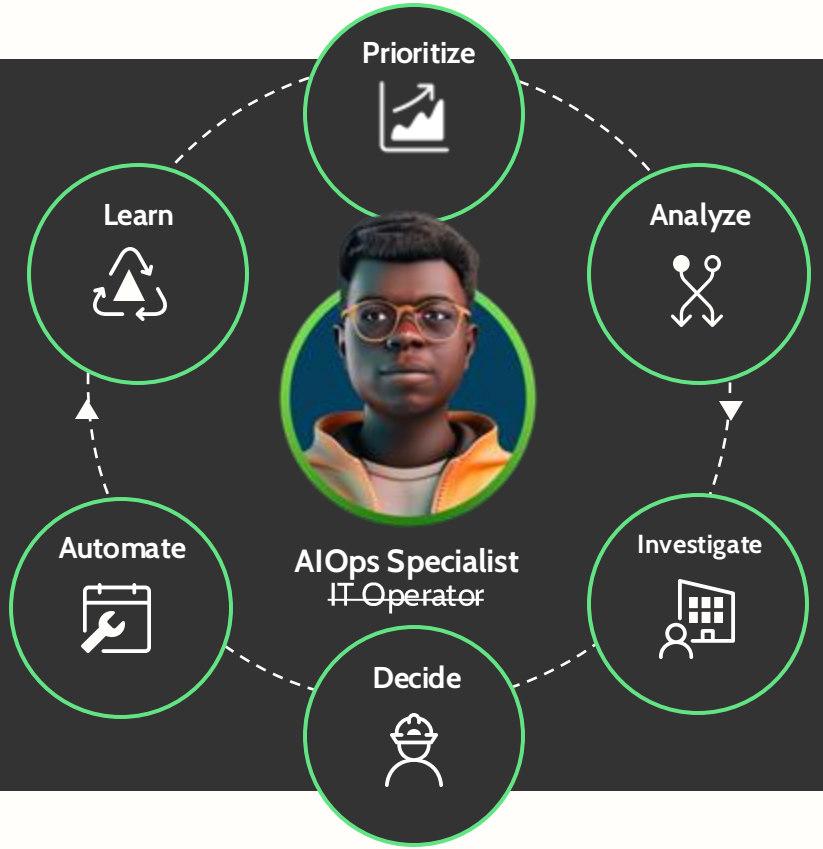
A team of AI Agents (internal and external) autonomously prioritizes key tasks, generates automation, and provides issue resolutions, while keeping operators informed and in control of decision-making.

IT operators shift from reactive firefighters to AI supervisors, increasing productivity and reducing MTTR

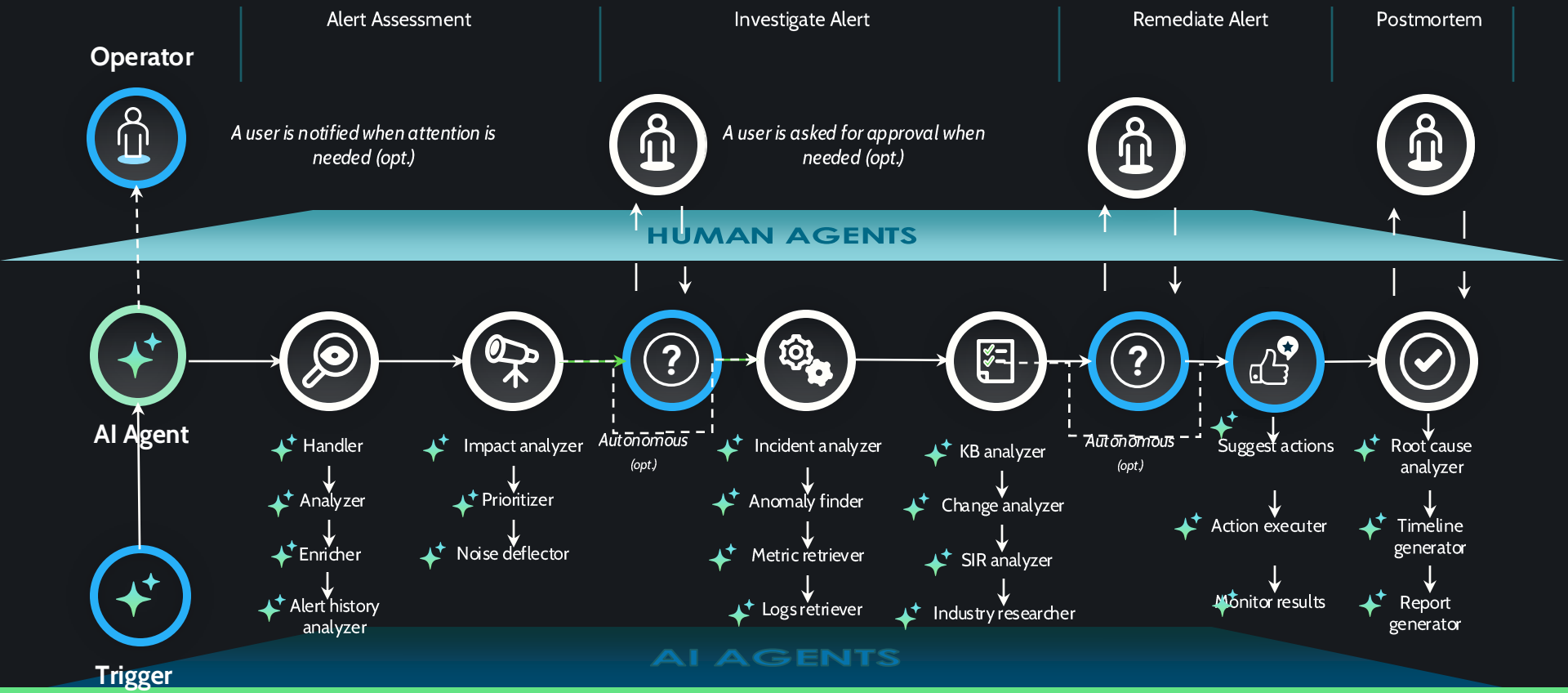
The Goal: Self Healing

The role of the Operator
Freed from repetitive tasks, operators oversee the AIOps Agent decisions, approve critical actions, and provide feedback.

Autonomous agent
Evolve from decision-support tools to autonomous responders, proactively detecting issues, implementing fixes, and continuously learning from operator feedback to refine future actions



Autonomous: AI Agent Drives, human is notified and approve



AUDIENCE POLL

How are you using AI today?

A. We use in-house LLM to help with business processes

B. We use AI companions built into our current tools (Copilot, Zoom companion, etc)

C. The usual conversational tools like ChatGPT, Gemini, DeepSeek, etc

D. We don't really "AI" today

Ondaro

Best Practices

Keys to Success

Executive Sponsorship	Realistic Targets	Completed prerequisites	Following Leading Practices	Good customer collaboration
• Consistent focus on the end value • Influence across the organization	• Activities and Timelines • Identified data sources and integration methods	• CMDB must be able to support desired functionality	• Target high-value (business critical; often cause incidents; shared infrastructure) areas first • Leverage existing customer processes to generate event and alert rules	• Access to SMEs – particularly Monitoring team resources • Tight integration between Incident and Event teams

Ondaro

Customer Success

Use Case - AI Ops

Reduction in Incidents through AI Ops Feedback

Problem Statement

JBOSS and WebLogic Performance Degradation

80% of alerts were being resolved with an engineer taking manual action on jBoss and Weblogic instances.

Engineer Work Performed:
This included

1. Reviewing alert
2. Opening a ticket
3. Logging into the remote machine instance and running resolution steps before an incident occurs.

Design

Design:

Reduce alert percentage and incident occurrence by utilizing AI Ops feedback from baseline behavior.

AI Ops provided feedback and gave options for resolution. Trends reviewed by team for next steps.

Outcome:

Used recommended baseline from Event Mgt metrics and root cause analysis: based on garbage collectors and peak size. Comparing it to a 30 day average. Alert Management kicked off a flow. Pulling in affected CI(s) and create a standard change request. Finally logging into the affected server and running remediation task.

Metrics Outcome

65%

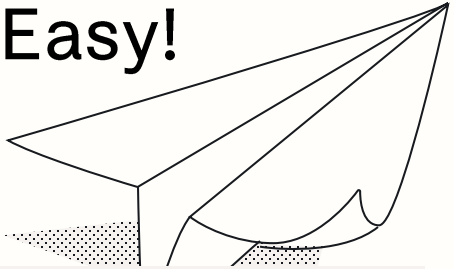
of alerts resolved

Process put in place to identify exceptions, included automation.

Root cause analysis used in Event Management and AI Ops Dashboard.

Getting Started Is Easy!

We can meet you where you're at in your Event Management journey.



Want a quick CMDB assessment and rapid remediation?

CMDB LAUNCHPAD

Need to implement CMDB and see value fast?

CMDB ESSENTIALS

Need a dedicated team for maintaining your ServiceNow Platform?

ONDARO RESERVE

Tell us what CMDB topics you want to learn more about!

Look for a survey following this session!

CMDB MasterClass Part 10:
Your CMDB Foundation for AI scheduled for November.

Look for an invite soon!

The next ITAM MasterClass: is on October 16.

Ondaro

Thank you!