



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

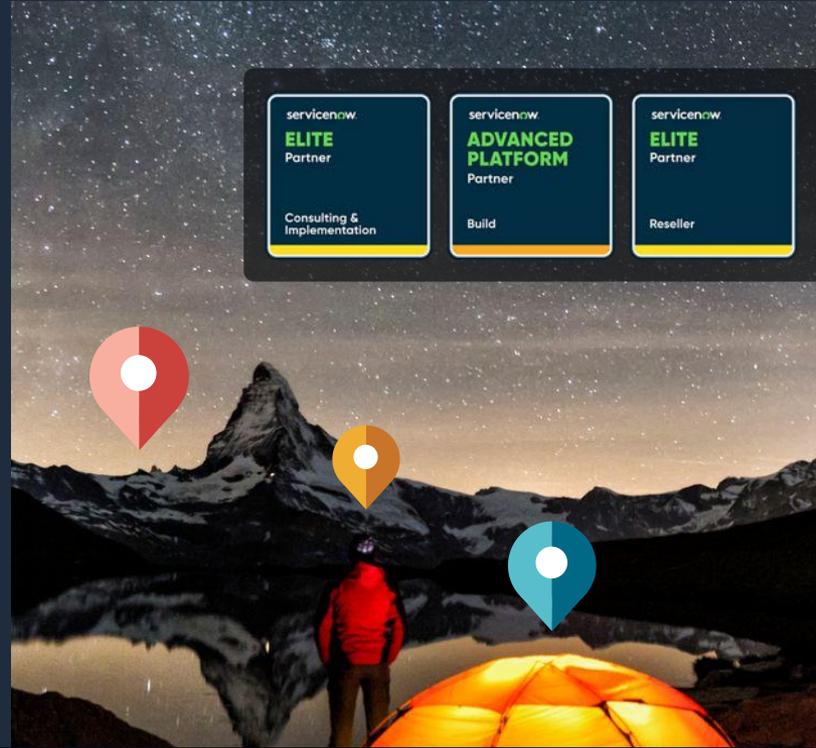




Cask NX is with clients for what comes next – on the platform and in their business.

4.6 Customer Satisfaction Rating

5.4K+ Certifications & Accreditations



<p>Validated Practice ✓</p> <p>IT Service Management AMS</p>	<p>Validated Practice ✓</p> <p>Customer Service Mgmt AMS</p>	<p>Validated Practice ✓</p> <p>Hardware Asset Mgmt AMS</p>	<p>Validated Practice ✓</p> <p>Software Asset Mgmt AMS</p>	<p>Validated Practice ✓</p> <p>ITOM Visibility AMS</p>	<p>Validated Practice ✓</p> <p>Vulnerability Response AMS</p>	<p>Validated Practice ✓</p> <p>Integrated Risk Management AMS</p>	<p>Validated Practice ✓</p> <p>Hybrid Project Mgmt AMS</p>
---	---	---	---	---	--	--	---

8 VALIDATED PRACTICES (Most of any Pure-Play Partner in AMS)

<p>Product Line Achievement</p> <p>Application Portfolio Management AMS</p>	<p>Product Line Achievement</p> <p>App Engine AMS</p>	<p>Product Line Achievement</p> <p>Human Resources AMS</p>
---	---	--

+3 PRODUCT LINE ACHIEVEMENTS

Cask NX is the only pure play ServiceNow partner with dedicated, fully certified practices across the platform.



IT SERVICE
MANAGEMENT



IT OPERATIONS
MANAGEMENT



IT ASSET
MANAGEMENT



STRATEGIC
PORTFOLIO
MANAGEMENT



EMPLOYEE
WORKFLOW



CUSTOMER
WORKFLOW



SECURITY
& RISK



APP ENGINE

STRATEGY

Strategic Roadmapping

Advisory Consulting

Platform Strategy &
Governance

Demand Management

TRANSFORMATION

App Modernization

UX & UI Design

Product Management

Org Change Management

Testing & Quality Engineering

Program & Project Management

Agile Transformation w/SAFe

IMPLEMENTATION & APP DEVELOPMENT

Product Implementation

Platform Engineering

Data Management &
Integrations

App Development

OPERATIONS & ENHANCEMENT

Continuous Cloud Innovation

Platform Architecture &
Engineering

Functional Process Execution

Cask Reserve

Introductions



Christine Morris
Director, ITx
Cask



Chris Padmore
Solutions Architect,
ITOM Practice Lead
Cask



Madan Raja
Director, Delivery
Cask

Join the Conversation: Using Zoom

Turn on Video

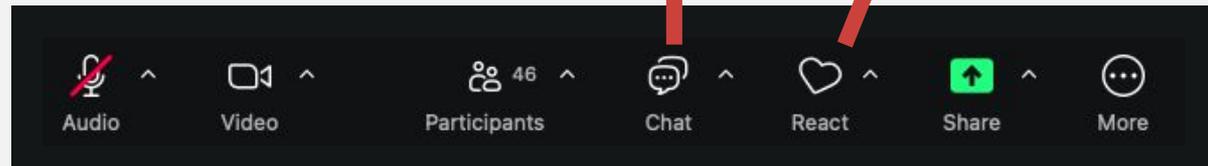
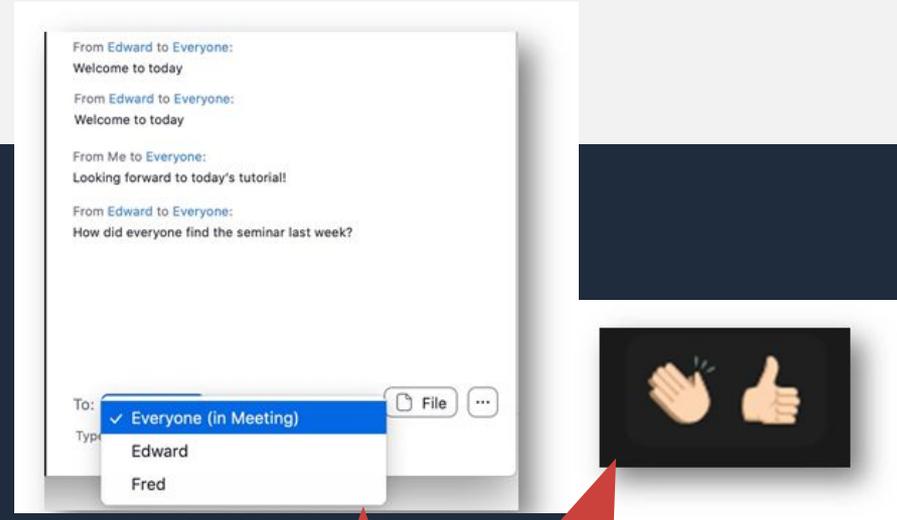
Let's get interactive and enjoy ourselves!

Unmute – Click the microphone icon to unmute and participate

Chat – Message everyone or just one person

Get Help – Use Chat

Show Captions - Click on MORE, click Show Captions



Catch Up with Parts 1-7 of our CMDB MasterClass Series!



Cask

CMDB FOUNDATIONS

Unlock the Power of Your Platform with a Strong CMDB Foundation

CMDB MasterClass

A thumbnail for the 'CMDB Foundations' masterclass. It features a man with curly hair and a beard, wearing a grey sweater, sitting at a desk and smiling. The background is a solid light orange color. The Cask logo is in the top left, and a red circular icon with 'CMDB MasterClass' is on the right.



Cask

CMDB & SECURITY

Maximize Your Platform's Potential with Effective CMDB Data Loading and IRE Strategies

CMDB MasterClass

A thumbnail for the 'CMDB & Security' masterclass. It features a man with glasses and a beard, wearing a blue button-down shirt, sitting at a desk with a laptop and smiling. The background is a solid light blue color. The Cask logo is in the top left, and a blue circular icon with 'CMDB MasterClass' is on the right.



Cask UNCSouthernCalifornia

CMDB & CSDM

Aligning Your CMDB to the CSDM Framework to Support your Portfolio of IT Services

CMDB MasterClass

A thumbnail for the 'CMDB & CSDM' masterclass. It features a woman with dark hair, wearing a grey blazer, sitting at a desk and talking on a mobile phone. The background is a solid yellow color. The Cask logo and 'UNCSouthernCalifornia' are in the top left, and an orange circular icon with 'CMDB MasterClass' is on the right.



Cask

CMDB & DISCOVERY

Maximize Your IT Potential: Discovery Meets CMDB

CMDB MasterClass

A thumbnail for the 'CMDB & Discovery' masterclass. It features a man with glasses and a beard, wearing a light blue shirt, sitting at a desk and looking towards the camera. The background is a solid dark blue color. The Cask logo is in the top left, and a red circular icon with 'CMDB MasterClass' is on the right.



Cask

CMDB & ITAM

A Strategic Approach to Visibility and Value

CMDB MasterClass

A thumbnail for the 'CMDB & ITAM' masterclass. It features a woman with glasses, wearing a blue blazer, holding a tablet and looking at it. The background is a solid light orange color. The Cask logo is in the top left, and a red circular icon with 'CMDB MasterClass' is on the right.



Cask

CMDB CARE AND FEEDING

Ongoing CMDB Maintenance: Feed It, Fix It, Love It

CMDB MasterClass

A thumbnail for the 'CMDB Care and Feeding' masterclass. It features a man in a dark suit, sitting at a desk with a laptop and smiling. The background is a solid light blue color. The Cask logo is in the top left, and a blue circular icon with 'CMDB MasterClass' is on the right.



Cask

CMDB & SERVICE MAPPING

From Chaos to Clarity: Mastering Service Mapping for CMDB Excellence

CMDB MasterClass

A thumbnail for the 'CMDB & Service Mapping' masterclass. It features a man with a beard, wearing a grey suit, standing with his arms crossed and smiling. The background is a solid dark blue color. The Cask logo is in the top left, and a red circular icon with 'CMDB MasterClass' is on the right.

Find recordings, resources & more here! <https://casknx.com/cmdb-masterclass-intro/>



Welcome to IT Operations



Welcome to IT Operations

Multiple Tools

Siloed Teams

Swivel Chair

Multiple Platforms

Disconnected Processes

Legacy Systems

Unexplained Outages





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.

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

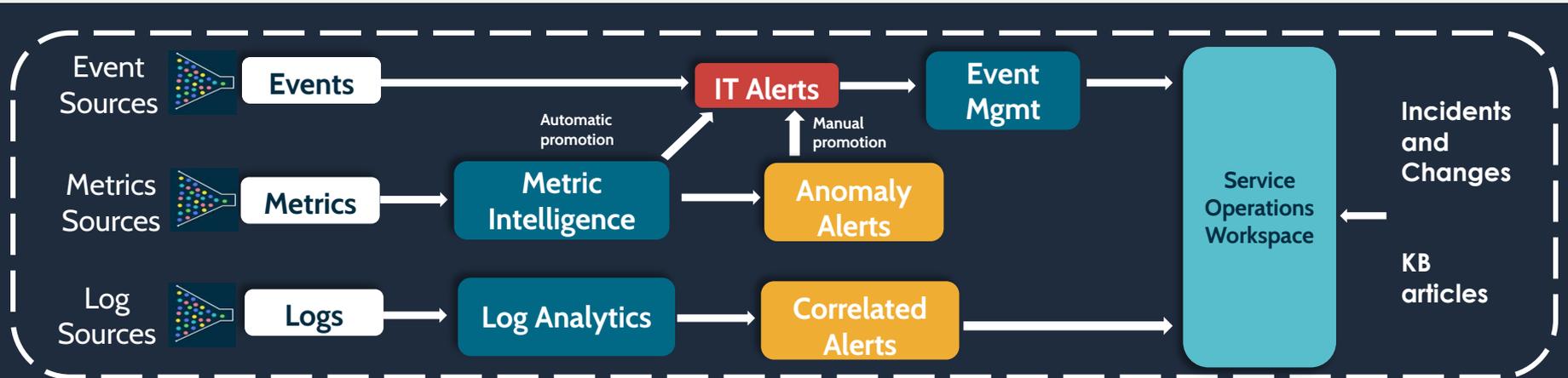
Incidents are derived from one or more unplanned events that negatively affect business services and require remediation

ITOM Health for events, metrics and logs

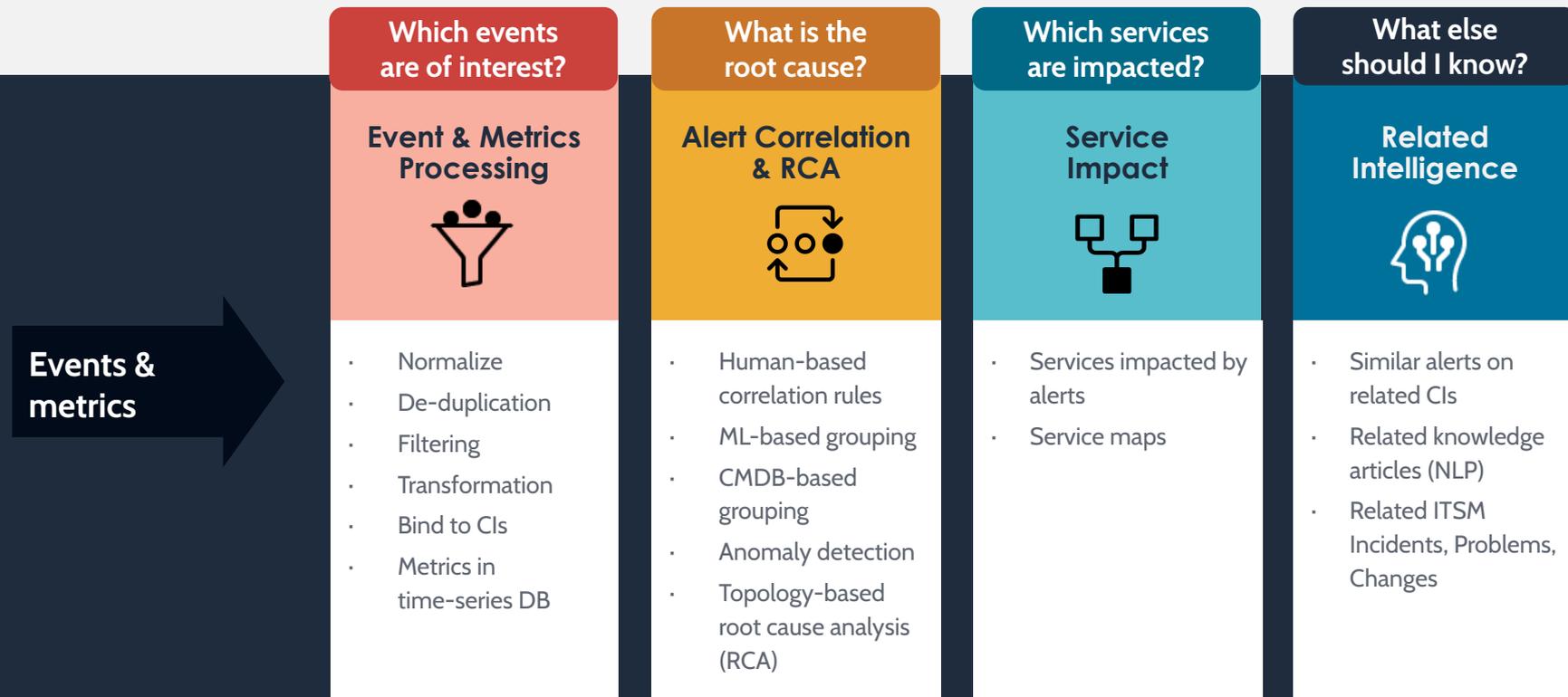
Event Management receives and processes events from external monitoring tools or from Agent Client Collector for Monitoring. Events are converted into alerts internally. Note: An alert in a monitoring tool (such as SolarWinds) is still considered an event in ServiceNow ITOM

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



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

Integrations launchpad

Bring together all of the events, metrics and logs from your infrastructure and get insights into the unified system.

[Browse integrations](#)

Installed integrations



🔍 All integrations ▾

Most popular

 Custom Connector(Webhook) Events	 Amazon Web Services Events	 Apache Metrics Metrics	 Docker Container Metrics Metrics	 Dynatrace Monitor Events	 Google Cloud Platform to instance Events
 Kafka Logs	 Microsoft Azure MID push Events	 Microsoft Azure to instance Events	 NagiosXI Events	 Nginx Monitoring Metrics Metrics	 SCOM Events
					

Review Data Faster

Express List +

Filters   [Save new](#)

Active Alerts(Default) 

 This filter was recently changed. [Update](#)

3 Applied conditions  [Clear all](#)

Fields 

- + State [Clear](#)
- + Updated
- + Severity [Clear](#)
- + Priority group
- + Source
- + Number
- + Configuration items
- + Impacted services
- + Node
- + Description
- + Assigned to
- + Assignment group

Active Alerts 4

[Close](#) 

<input type="checkbox"/>	Number	Description	Duration 	Severity
<input type="checkbox"/>	Alert0088580	Certificate is about to expire	2 weeks ago	Warning
<input type="checkbox"/>	Alert0088569	Current status of MID midserver_acc extension is Offline. Ensure the MID server...	3 weeks ago	Minor
<input type="checkbox"/>	Alert0088563	There is an error in the MID server - midserver_acc: User midserver associated wi...	1 month ago	Minor
<input type="checkbox"/>	> Alert0088562 2	Group of alerts, The following Distributed Clusters are in the following states: Cluster:...	1 month ago	Major

Manage Services Easier

Service Dashboard

Alert0088562

Alert0088580

Default | 8 services

Severity breakdown  2 critical 25.0%  0 major 0%  0 minor 0%  0 warning 0%  6 ok 75.0%

Group by **Business criticality** ▼

Group order **Ascending** ▼

Segment each group by **Severity** ▼

Home

1 - most critical (8)



Libor Controls Processing

Mortgage Calculator



Payments Platform

Asset Reconciliation

Financial Audit

IT Service Management
PROD

+2

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

AI Ops Overview

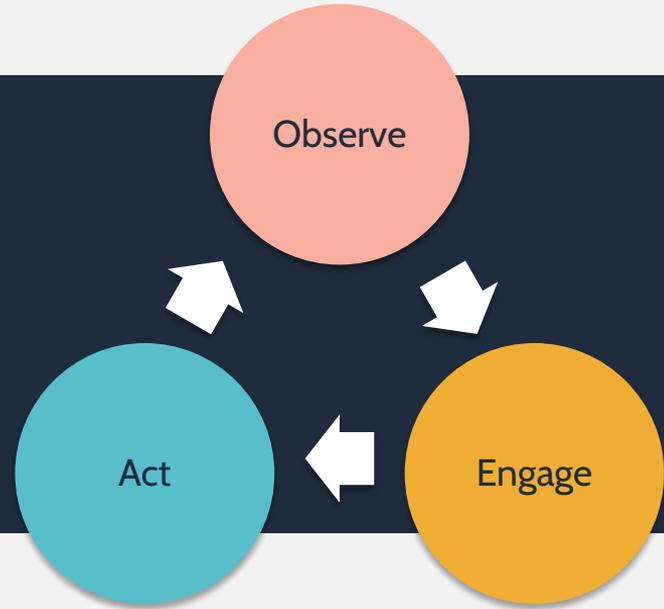


AIOPs Approach

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-off automated self-healing

AIOps Workspace

AIOps Operational ▾

Certified



Edit



Events and Alerts

HLA Operational

Trends

Noise reduction (events to alerts compression)



55.00%

↓ -0.56% (-1.0%) since May 29



Alerts grouping coverage



13%

↓ -6% (-30.8%) since May 29



Incident compression rate



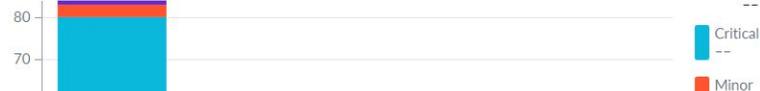
100%

— 0% (0.0%) since May 29

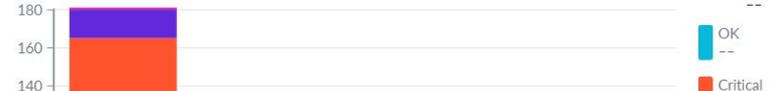


Outcomes

Top 20 alert sources (last 7 days)



Top 20 event sources (last 5 days)



Now Assist for ITOM

✦ Alert analysis generated by Now Assist ⓘ



Summary:

- MID Server Role Not Associated with a MID Server
- The MID server role 'lab.midserver' is not associated with an actual MID Server. This means that there is no MID Server currently running with this role.

Analysis:

This situation could potentially impact the functionality of the MID Server, as it is not properly associated with a role. It is recommended to first verify if there is indeed a MID Server with this role that is not running or properly configured. If no such MID Server exists, it may be necessary to remove the role or associate it with a functioning MID Server. Additionally, it would be prudent to investigate the reason why no login attempts were recorded within the reporting period.



Updated 2025-06-04 23:42:32

Be sure to check AI-generated content for accuracy.

AUDIENCE POLL

Who manages your alerts today?

- (A) Each monitoring team handles their own alerts

- (B) Each application team handles their own alerts

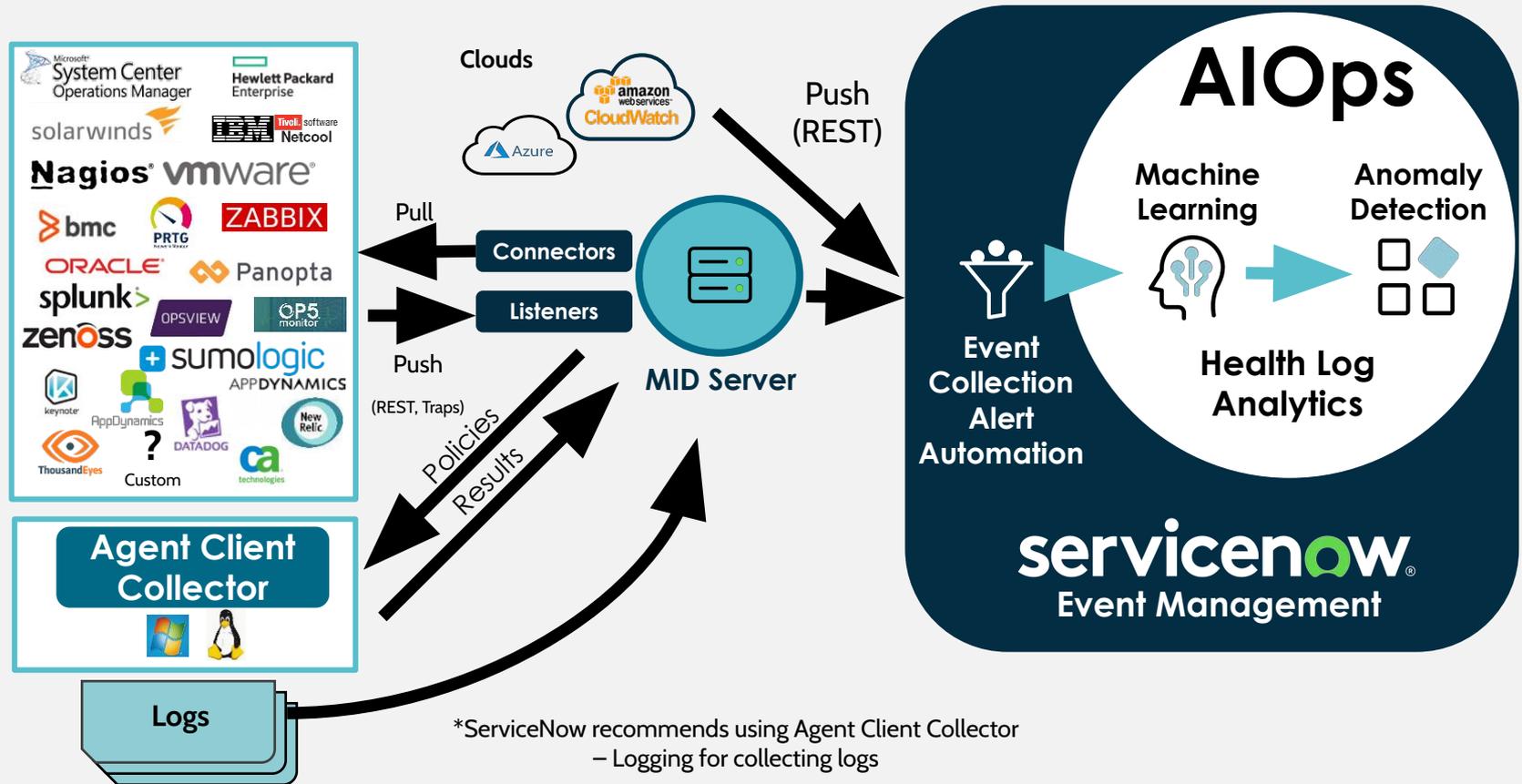
- (C) We have a centralized response team that handles all alerts

- (D) We've never resolved an alert

Putting it all together Event Management & AIOps



Event Management and Health Log Analytics



ITOM AIOps Agents persona



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

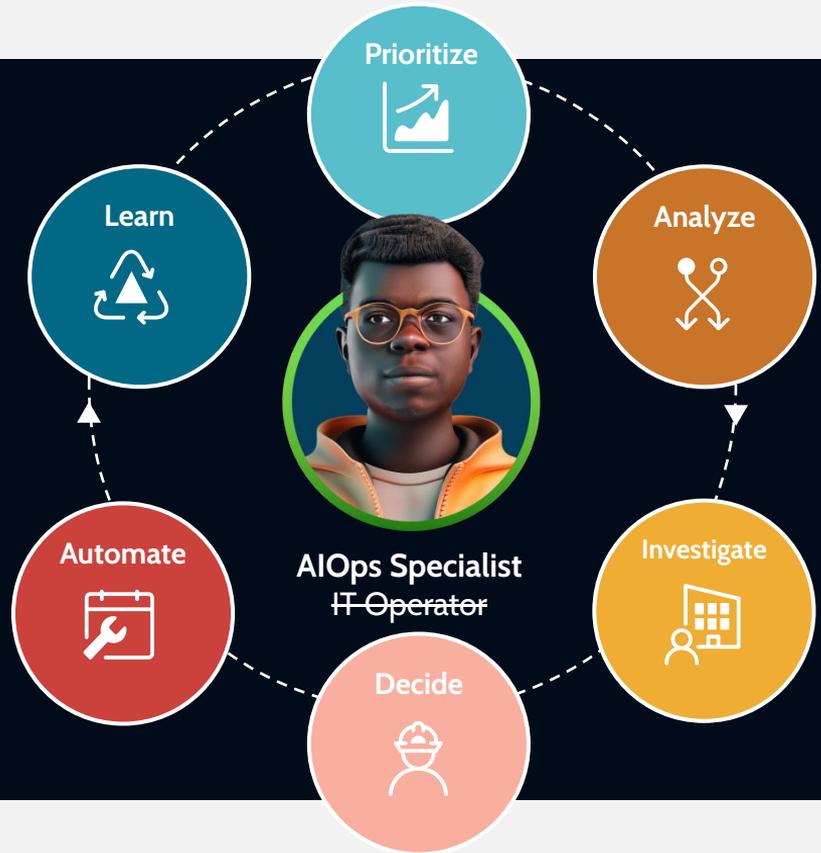
The Goal: Self Healing

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

Best Practices



Keys to Success

1

Executive Sponsorship

- Consistent focus on the end value
- Influence across the organization

2

Realistic Targets

- Activities and Timelines
- Identified data sources and integration methods

3

Completed prerequisites

- CMDB must be able to support desired functionality

4

Following Leading Practices

- Target high-value (business critical; often cause incidents; shared infrastructure) areas first
- Leverage existing customer processes to generate event and alert rules

5

Good customer collaboration

- Access to SMEs – particularly Monitoring team resources
- Tight integration between Incident and Event teams



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

Ready to get started with Event Management?

Event Management
Implementation

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

Look for a survey following this session!

Join our next **ITAM MasterClass** on June 26.



CMDB MasterClass Part 9:
Vulnerability Management is
scheduled for July 16.
Look for an invite soon!

Questions?





Thank you!

Email: Madan Raja, madan.raja@caskinc.com

