

APEX AIOps Incident Management

KI-gesteuerter Incident-Lebenszyklus-Workflow zur Optimierung der Verfügbarkeit der digitalen Infrastruktur

99 % weniger Ereignisrauschen¹

50 % weniger Tickets¹

93 % weniger von KundInnen gemeldete Probleme¹

Reduktion von Ereignisrauschen reduziert Millionen von Raw-Ereignissen auf Tausende eindeutige Warnmeldungen.

Warnmeldungskorrelation korreliert Tausende von Warnmeldungen zu einzelnen, umsetzbaren Incidents mit wahrscheinlicher Ursache.

Echtzeit-Situationseinblicke erkennen proaktiv geschäftliche Auswirkungen, während sich Incidents entfalten.

Teambasierter Workflow für die Zusammenarbeit optimiert die Kommunikation zwischen Teams und Tools mithilfe des Situation Room.

Algorithmisches Wissen erfasst und kodifiziert Erfahrungswerte aus früheren Incidents für die Wiederverwendung, z. B. wie frühere Incidents gelöst wurden

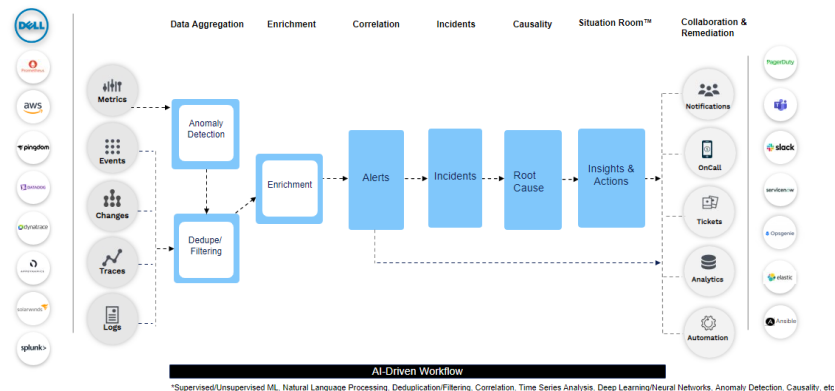
ITSM- und Runbook-Integration löst durch die Integration in IT-Tools von Drittanbietern Tickets, Eskalation und Korrektur aus.

Die Sicherstellung der Verfügbarkeit Ihrer digitalen Infrastruktur wird schwieriger, da Ihre Anwendungs-, Daten-, Compute-, Storage- und Netzwerkressourcen über Rechenzentren, Edge-Standorte und die Cloud hinweg skaliert werden. Events und Warnmeldungen von Monitoring-Tools in allen Technologiebereichen erschweren es IT-Betriebs-, DevOps- und SRE-Teams, die Ursache von Incidents zu ermitteln, und behindern die Behebung, während Ihre KundInnen, MitarbeiterInnen und Ihr Unternehmen darunter leiden.

Zur Bewältigung dieser Komplexitäten benötigen Sie eine KI-gesteuerte Lösung.

APEX AIOps Incident Management, Teil der APEX AIOps Software as a Service, automatisiert die Verfügbarkeit Ihrer digitalen Infrastruktur durch automatisierte, KI-gesteuerte Incident-Lebenszyklus-Workflows.

Es nimmt Daten aus all Ihren IT-Tools unterschiedlicher Anbieter auf und nutzt KI, um Events und Warnmeldungen in einzelne umsetzbare Incidents zu reduzieren, wahrscheinliche Ursachen zu identifizieren und die relevanten MitarbeiterInnen zu mobilisieren, damit sie zielgerichtet zusammenarbeiten und Vorfälle schneller beheben können.



Automatisierter Workflow für das Incident Management: Wandelt Störgeräusche in umsetzbare Incidents um und rationalisiert die Zusammenarbeit und Korrektur für eine schnellere Lösung von Problemen, die sich auf den Service auswirken.

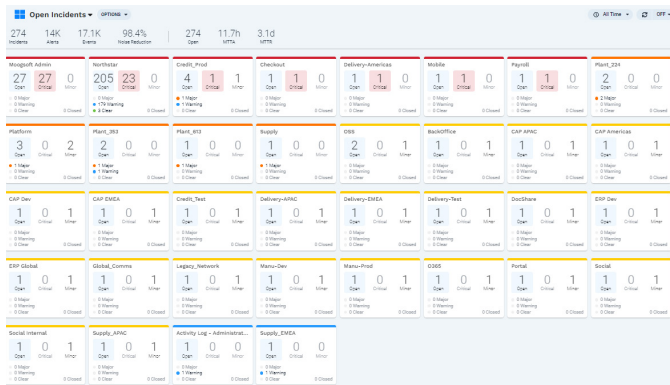
Reduktion von Warmmeldungsrauschen und umsetzbare Einblicke in Incidents, die sich auf den Service auswirken

Incident Management ist in mehr als 100 gängige IT-Monitoring- und Managementtools von Drittanbietern vorab integriert und nutzt maschinelles Lernen (ML) in Echtzeit und andere KI-Algorithmen, um die Relevanz und die Beziehungen der aufgenommenen Betriebsdaten zu ermitteln. Eine einfach zu bedienende Benutzeroberfläche ermöglicht es Ihnen, zusätzliche Integrationen selbst durchzuführen.

Wie im Workflowdiagramm auf Seite 1 dargestellt, erkennt das Incident-Management Filter und verwirft eingehende Low-Level-Events wie Heartbeat-Signale und dedupliziert die übrigen folgenschweren Events wie den Ausfall einer Hardwarekomponente oder Ereignisse im Zusammenhang mit der Anwendungslatenz, die eine Aktion erfordern. Dadurch werden Millionen von Events (sowie Änderungen, Ablaufverfolgungen, Protokolle und Anomalien) in Tausende von eindeutigen, wichtigen Warmmeldungen reduziert.

Als Nächstes stellt eine algorithmische Korrelations-Engine, die sowohl unüberwachtes als auch überwachtes maschinelles Lernen einsetzt, Beziehungen zwischen Warmmeldungen und ihren Attributen für bestimmte geschäftliche Auswirkungen her und fasst sie zu einem einzigen Incident zusammen.

Incidents werden in Echtzeit erstellt, während sie sich in der Produktion weiterentwickeln, und Algorithmen clustern ähnliche Incidents, um das Rauschen weiter zu reduzieren.

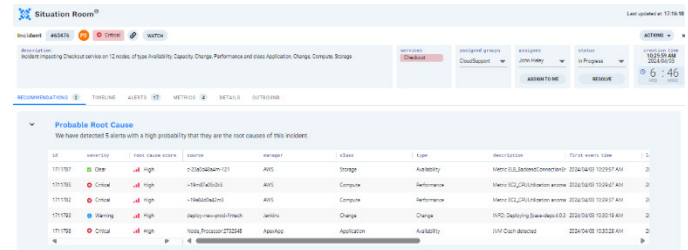


Echtzeit-Dashboard: Nutzerdefinierte Dashboards bieten einen sofortigen Einblick in den aktuellen Status von Incidents im gesamten Unternehmen. Dashboards lassen sich leicht an die individuellen Anforderungen von Operations Center, DevOps, SRE, Server, Storage, Netzwerk oder anderen Teams sowie von Geschäftsbereichsinhabern oder anderen Führungskräften anpassen.

Schnellere Ermittlung der Ursache

Kausalitätsalgorithmen identifizieren Änderungen an kritischen Nodes in physischen und logischen Topologien, um die Auswirkungen von Warmmeldungen zu bewerten und zu verstehen. Überwachtes und nicht überwachtes ML analysiert Muster, frühere Incidents und Zeitskalen, Nähe und sprachliche Aspekte von Warmmeldungen sowie Änderungen, um die wahrscheinlichste Ursache für jeden Incident zu identifizieren.

Mit der Option „Wahrscheinliche Ursache“ werden wichtige Warmmeldungen als Hauptursache identifiziert, anstatt dass NutzerInnen potenziell Hunderte von Warmmeldungen analysieren müssen.

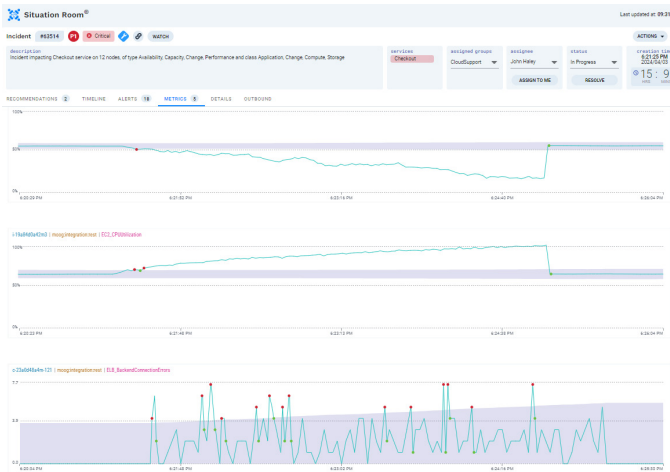


Wahrscheinliche Ursache: Auf der Grundlage des trainierten Modells zeigt der Algorithmus eine oder mehrere Warmmeldungen im Zusammenhang mit dem Incident als wahrscheinliche Ursache an, um den Korrekturprozess zu beschleunigen.

Beseitigung von Silos, Verbesserung der Zusammenarbeit und Beschleunigung der Problemlösung

Das Herzstück von Incident Management ist ein kollaborativer Workflow, der aus einem Incident automatisch ableitet, welches Team benachrichtigt werden sollte, und dieses an den Situation Room weiterleitet. Hierbei handelt es sich um einen virtuellen Raum, in dem Fachexperten und andere Stakeholder zusammenarbeiten und Incidents effizient lösen können, indem sie den Incident, die wahrscheinliche Ursache sowie die Zeitskala und die Details der Warmmeldungen untersuchen.

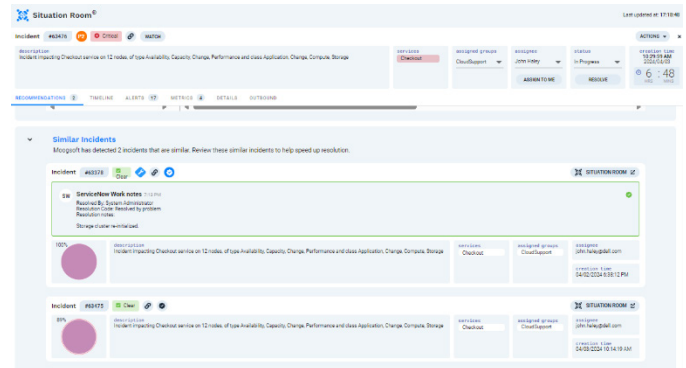
Algorithmen vergleichen aktuelle und vergangene Incidents. Durch die Zuweisung eines Ähnlichkeitsprozentsatzes für jeden Incident können Teams Ratschläge zur Behebung ähnlicher Incidents anzeigen und befolgen. Teams können auch wiederkehrende Probleme identifizieren, da Algorithmen die nötigen Erkenntnisse liefern, um schädliche Auswirkungen auf Geschäftsservices zu verhindern, bevor sie auftreten.



Kennzahlen für Zeitreihen: Für tiefere Einblicke werden Anomalien im Zusammenhang mit jeder Kennzahl von unten nach oben angezeigt, von der Warnmeldung der wahrscheinlichen Ursache bis hin zu kaskadierenden symptomatischen Warnmeldungen.

Time	Action	By
6:02:02 AM	Confirming the service is restored	Johanna
6:02:15 AM	Update team assignment	Johanna
6:02:25 AM	Trying to restart storage cluster	Johanna
6:04:47 AM	Save file to storage issue	Johanna
6:08:18 AM	Looking into the issue	Johanna
6:09:01 PM	Status changed to Sub-critical	Johanna
6:09:01 PM	Status changed to Sub-critical	Johanna

Zeitskalen und Details: Zusätzliche Einblicke bietet eine Zeitskala mit Kommentaren von Teammitgliedern, ergriffenen Maßnahmen, Ergebnissen, Zuweisungsänderungen und mehr.



Ähnliche Incidents und Empfehlungen: Historische, ähnliche Vorfälle sowie die Schritte zur Lösung werden für jeden neuen Incident angezeigt. Diese Lösungsschritte können manuell oder programmgesteuert mithilfe der API angewendet werden, um das Problem zu beheben, das den Incident verursacht.

Automatisierung von ITSM, Eskalation und Lösung von Incidents

APEX AIOPs Incident Management ist in viele gängige ITSM-Tools (z. B. ServiceNow, Remedy, Jira) vorab integriert, um umsetzbare Servicetickets zu initiieren. Es bietet weiterhin Kommunikationstools (z. B. PagerDuty, Slack, Microsoft Teams) für Benachrichtigungen und zur Eskalation von Maßnahmen sowie Automatisierungstools (z. B. Ansible, Terraform) zur Automatisierung von Korrekturmaßnahmen.

Die Korrektur kann automatisiert werden oder manuell erfolgen, wenn eine fortlaufende Genehmigung erforderlich ist.

Weitere Informationen finden Sie unter www.dell.com/apex-aiops.



[APEX AIOPs-Produktübersichten](#) lesen



[Demo zu APEX AIOPs](#) ansehen



Dell Experten [kontaktieren](#)



Jetzt mitreden:
#DellAPEX
#AIOPs

¹Kundenumfrage, Moogsoft, 2024. Die tatsächlichen Ergebnisse können abweichen.