NEW WAVE OF INNOVATIONS IN BMC HELIX AIOPS AT CONNECT 2024

Inefficiency and increased vulnerability due to visibility gaps in IT operations (ITOps) and security operations (SecOps) can leave IT teams constantly playing catch up. The BMC Helix AIOps release for BMC Connect 2024 aims to solve these challenges, all while improving the overall operator experience with BMC HelixGPT. Bringing together service management, observability, and vulnerability data, and using integrated workflows and automations to streamline incident response and risk management, BMC Helix enables teams to collaborate and resolve problems before they impact the business.

BMC Helix AIOps: Respond proactively to incidents and outages with a lot less effort

Proper use of artificial intelligence (AI), including causal, predictive, and generative AI (Gen AI) for smart assistance, can speed up incident resolutions and boost productivity. The latest release of BMC Helix AIOps enhances troubleshooting workflows and enriches the operator experience by introducing the BMC Ask HelixGPT virtual assistant, which helps IT operations teams get answers to common troubleshooting questions using predefined prompts. The log insights surfaced to DevOps and site reliability engineering (SRE) teams enable them to identify unusual behaviors in log data, without having to manually sift through thousands of log entries. The chat-mode interface makes it easy to get to the root cause faster, thereby reducing mean time to repair (MTTR). Altogether, the

solution eliminates war-rooms by helping teams:

- Reduce manual investigation work with an AI assistant that retrieves answers to commonly asked questions during troubleshooting.
- Act rapidly by understanding impacts with topology, root cause isolation, situation explanation, and change risk prediction, all in a business context.
- Eliminate manual troubleshooting with logs and resolve incidents faster by identifying unusual behaviors in log data.

The addition of new, synthetic session data, Netreo events, and Stackify metrics allows BMC Helix AIOps to advise specific actions based on more complete data.

ServiceOps: Balance speed and risk in DevOps

For organizations practicing ServiceOps to balance speed and risk in service and operations management (ITSM/ITOM), the enhanced integration with ITSM systems allows BMC Helix AIOps to initiate workflows and create incident tickets from AIOps-created situations, thereby reducing incident noise and costs. The integrated ITSM and AIOps workflows streamline incident management and eliminate context switching by cross-launching between BMC Helix AIOps and ITSM systems from BMC and ServiceNow.

The most effective way to manage change and its impact is to proactively analyze risks to avoid making changes that are likely to cause an incident. The current change management process typically involves manual analysis of risk and lacks real-time operational data for accurate risk predictions. The new Gen AI-powered change risk advisor in BMC Helix AIOps reduces change failures in complex systems by surfacing risky changes that help users analyze change requests that may impact the service. Using Ask BMC HelixGPT, DevOps and SRE teams can follow up with questions and get responses for a given change request so they can continue to deploy quickly and with confidence, only delaying their push when a potential failure is detected.

By journeying towards ServiceOps, IT teams will:

- De-risk DevOps by catching unforeseen risks in real time and using BMC Ask HelixGPT to ask questions around a given change request.
- Prevent and identify risk changes with more precise risk and impact analysis of ITSM/ITOM data.
- Reduce incident noise and costs through integration with ITSM, allow BMC Helix AIOps to initiate workflows and create tickets from situations.

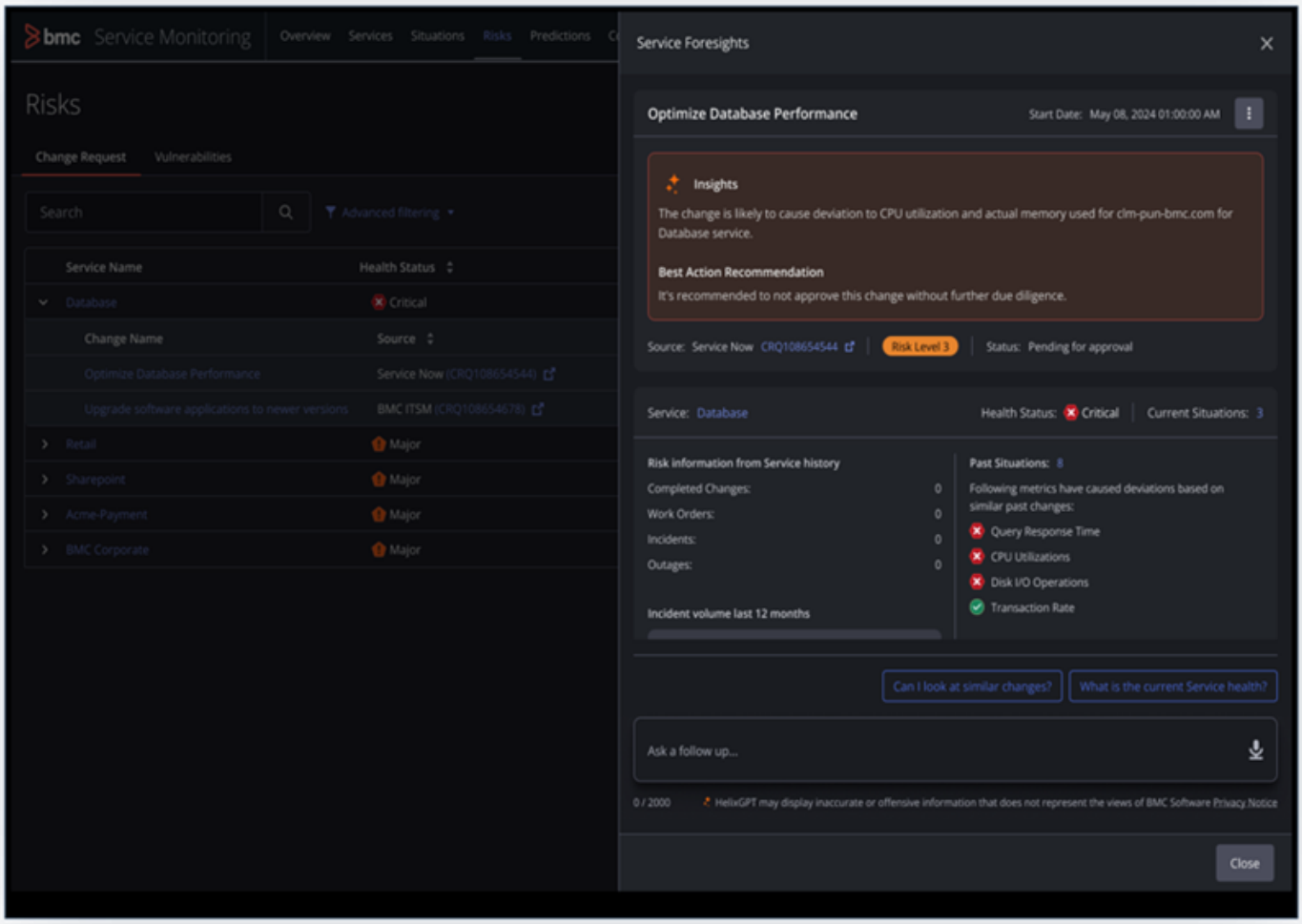

Figure 1. Gen AI-powered change risk advisor in BMC Helix AIOps.

VulnOps: Resolve exposures faster with risk and impact analysis

Automation is crucial to improving operational efficiency and driving faster vulnerability incident response. More and more vulnerabilities come out every day and operators are not fast enough to identify solutions for them. For ITOps and SecOps teams, new vulnerability scanning capabilities in BMC Helix AIOps enhance the visibility of risks with the context of the services impacted. With service vulnerability risk, organizations get protection through continuous scanning and monitoring of the organization's assets and potential risks.

Vulnerability best action recommendation (VBAR), another key capability in BMC's vulnerability operations (VulnOps) solutions, uses BMC HelixGPT to reduce the noise in vulnerability management and accelerate automated responses with code generation, so ITOps and SecOps teams can meet regulatory compliance and internal policies and procedures. With these combined capabilities, organizations can:

- Focus on the severe vulnerabilities through visibility into services and owners with the highest level of vulnerability risks.
- Speed vulnerability remediation by identifying the required patch or potential workaround for each vulnerability using AI-powered VBAR.
- Reduce noise in vulnerability management and prioritize the real risks so teams know what,

where, and how to fix the issue.

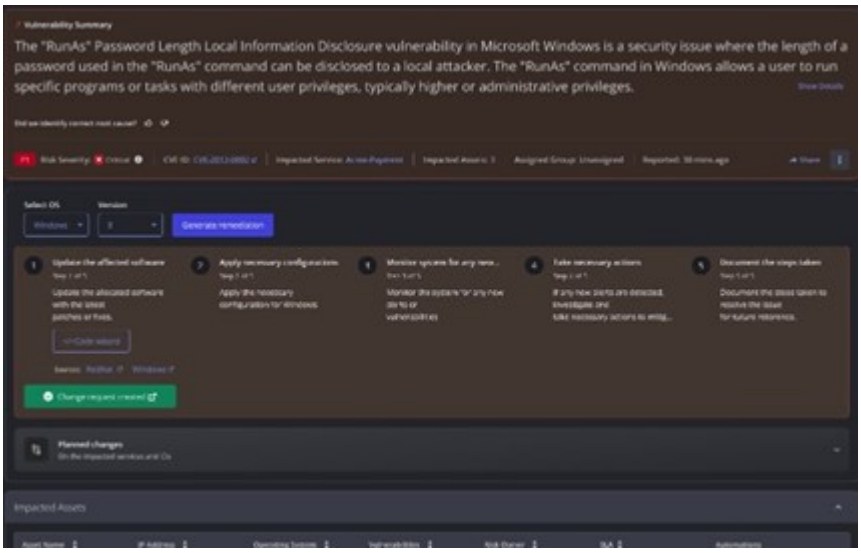

Figure 2. Gen-AI powered VBAR in BMC Helix AIOps.

BMC Helix Discovery: Gain visibility of complex networks, containers, and cloud resources

Enterprises deploy complex network topologies using various protocols. Border Gateway Protocol (BGP) is one of the most used protocols to build logical connectivity across network devices within and across datacenters. In the latest BMC Helix Discovery release, IT and networking teams can discover complex network topologies using BGP to gain comprehensive network visibility across their infrastructure to improve network troubleshooting and help BMC Helix AIOps provide holistic, accurate root cause correlation. Other BMC Helix Discovery enhancements include:

- Deep container discovery, which enables IT teams to understand the software running inside containers and the impact on services from outages within the cluster.
- Implicit discovery scanning in Microsoft Azure and Oracle Cloud Infrastructure (OCI), which uses existing cloud API scans and credentials to discover all components of running cloud servers.

Netreo: Accelerate network troubleshooting with improved efficiency

Since the BMC acquisition of Netreo and Stackify earlier this year, we've been busy with integration work to consolidate data for end-to-end visibility and AIOps. Customers using Netreo and Stackify will be able to ingest events and metric data into the BMC Helix platform through intelligent connectors. This data will be useful for unified monitoring and enabling AIOps use cases such as root cause analysis and incident resolution.

To accelerate network troubleshooting, Netreo Path Insights turns every possible connection route into a visual histogram backed with deep performance statistics. This capability reduces MTTR by enabling IT teams to quickly track and resolve remote performance issues with color-coded network mapping and an intuitive user interface.

Additional enhancements

Other new enhancements include advanced reporting with BMC Helix Dashboards in BMC Helix Continuous Optimization, which simplifies reporting and auditing for capacity management by providing the ability to manage basic and advanced reports in one place. IT teams can schedule, distribute, and archive reports with proper access control.

We're continuing to optimize how ITOps and SecOps teams interact with our AIOps solution. Whether through integrated workflows, intelligent integrations, deep network and container discovery, or security vulnerability automation, each update aims to improve IT and security operational visibility and efficiency. To learn more about the BMC Ask HelixGPT virtual assistant, change risk advisor or our VulnOps solution, contact us for a consultation.