HOW AGENTIC AI CAN ALLEVIATE VULNERABILITY RISKS FOR SECOPS

Security and IT operations (SecOps) teams face serious fatigue dealing with rapidly evolving threats. Traditional vulnerability management requires too many manual tasks before finding a fix as SecOps teams can take weeks and even months to review documentation, make recommendations, and coordinate vulnerability patches. That's a lot of time for an attacker to exploit vulnerabilities and potentially compromise your organization's systems and data.

The real problem is that most security teams don't have enough knowledge about what's running in their IT and DevOps environments to understand, prioritize, and fix critical vulnerabilities. When the list of vulnerabilities gets passed on to the IT operations (ITOps) and DevOps teams, they often don't know how to remediate the vulnerability, so they must manually investigate the proper remediation steps.

How agentic AI can help

Generative artificial intelligence AI (GenAI) and agentic AI can help SecOps teams transform their approach to vulnerability management by shortening the time to resolve exposures, improving compliance and risk management, and collaborating on ways to fortify business resiliency. According to BMC's recent *State of GenAI and Agentic AI for IT* report:

- 49% of respondents want AI to detect, prioritize, and resolve vulnerabilities

- 43% see automated vulnerability risk resolution in their future

BMC HelixGPT Vulnerability Resolver is an AI assistant within the BMC Helix AIOps and Observability solution suite that helps SecOps teams quickly address vulnerabilities through risk and impact analysis, task automation, and remediation recommendations. By consolidating vulnerability data, the BMC HelixGPT Vulnerability Resolver provides a comprehensive view of the vulnerabilities that are affecting critical business services and presents the risk and impact side by side with service health. This allows teams to identify the services and owners with the highest levels of vulnerability risks that demand rapid remediation or attention.

To assist teams in responding swiftly, the AI assistant offers a summary of each vulnerability from the Common Vulnerabilities and Exposures (CVE) list, along with a link to full details. Most importantly, the BMC HelixGPT Vulnerability Resolver recommends actions for addressing each critical vulnerability. If code changes are needed for remediation, the code wizard will provide the required code change. With a click, ITOps and DevOps teams can use the remediation steps provided by the AI assistant to create a change request for each affected asset that also includes pertinent information about the vulnerability.

How agentic AI can transform vulnerability management

As AI assistants evolve, understanding and harnessing their full potential can help transform vulnerability management. And assistants that combine machine learning (ML) with specialized domains like causal and predictive AI could drive even greater efficiency and autonomy for SecOps teams.

BMC Helix AIOps integrates causal, predictive, and generative AI to analyze observability data, identify the root cause, and access the impact an incident has on services. The solution's predictive AI scans for non-obvious trends in the data to detect impending and ongoing issues, while causal AI correlates and causally associates anomalies. When the solution detects a critical situation that requires a deeper dive, agentic AI can identify scenarios like the risks associated with vulnerabilities and security threats by pulling just-in-time data processed with GenAI.

The BMC Helix AIOps solution increases collaboration between ITOps and SecOps, enabling teams to share responsibility for identifying and quickly resolving security vulnerabilities. With the BMC HelixGPT Vulnerability Resolver assistant, SecOps will understand the impact on business services, which helps them prioritize and resolve critical vulnerabilities faster.

Watch the BMC HelixGPT Vulnerability Resolver demo to see agentic AI in action, and contact us for a consultation.