Publicado en Madrid el 09/07/2021

BMC refuerza la seguridad del mainframe con nuevas prestaciones frente a amenazas maliciosas internas

BMC, un líder mundial en soluciones de software para Autonomous Digital Entreprise (ADE), anuncia varias innovaciones e integraciones en su oferta BMC Automated Mainframe Intelligence (BMC AMI) y BMC Compuware dirigidas a mejorar la detección de amenazas y la respuesta ante ellas, y a ampliar el acceso a las principales herramientas DevOps para aumentar la productividad de los desarrolladores. Estas propuestas ayudan a las empresas a automatizar y gestionar flujos de trabajo con facilidad y agilidad

BMC, un líder mundial en soluciones de software para Autonomous Digital Entreprise (ADE), anuncia varias innovaciones e integraciones en su oferta BMC Automated Mainframe Intelligence (BMC AMI) y BMC Compuware, dirigidas a mejorar la detección de amenazas y la respuesta ante ellas, y a ampliar el acceso a las principales herramientas DevOps para modernizar las aplicaciones de mainframe y aumentar la productividad de los desarrolladores.

Estas novedades permiten al usuario:

Detectar los puntos débiles y la actividad maliciosa antes de correr riesgos mediante la detección y respuesta automatizadas ante un acceso privilegiado sospechoso o inusual.
Acelerar el rendimiento del equipo de desarrollo con nuevas integraciones que simplifican los canales de integración continua (CI) y entrega continua (CD), además de coordinar los despliegues automatizados desde distintas plataformas.
Aumentar el rendimiento y la resiliencia del mainframe con una solución que diagnostique los posibles problemas de funcionamiento de Java Virtual Machine (JVM), una prestación importante teniendo en cuenta que cada vez existen más aplicaciones Java en mainframes.
Mejorar la experiencia del desarrollador de mainframe y el programador de sistemas mediante la contribución al proyecto Zowe de mainframe abierto.

Acceso protegido a cuentas privilegiadas
La ruta más rápida hacia los datos de un mainframe son las cuentas privilegiadas, así como las actividades del supervisor y las credenciales con nombre. Estas cuentas pueden verse en peligro debido a ataques externos o usos internos maliciosos que pueden emitir actividades que les permitan acceder y robar información valiosa. Peor aún, una vez en peligro, representan una manera eficaz para que los atacantes desplieguen ransomware, eviten la detección e incrementen su tiempo de exposición.

El nuevo y ampliado detector de llamadas y el enriquecimiento de datos de Unix® System Service (USS) para la solución BMC AMI Security muestra las llamadas que podrían indicar una actividad

maliciosa y expone rápidamente las acciones de los usuarios con privilegios de superusuarios. Esta solución otorga a todos los clientes de BMC AMI Security un nivel añadido de seguridad ante los riesgos para cuentas de usuarios privilegiados a fin de detener y prevenir las amenazas, los robos internos o los niveles de privilegio inadvertidos que podrían desembocar en ataques futuros.

Según Forrester[1], “tanto si son accidentales como si son maliciosos, los incidentes internos pueden generar fraude financiero, violación de la privacidad, robo de la propiedad intelectual o daños a infraestructuras. Para los expertos en seguridad es difícil detectar esta actividad sospechosa porque las personas necesitan tener acceso privilegiado a datos para hacer su trabajo. Puesto que estas personas tienen derecho a la confidencialidad y las garantías procesales, los expertos en seguridad deben gestionar estos incidentes con mucho más cuidado que si se tratase de amenazas externas”.

Incrementar la agilidad del desarrollador y actualizar las aplicaciones con mayor rapidez
BMC sigue ampliando el acceso a herramientas habilitadas por DevOps para desarrolladores de mainframe de todos los niveles de experiencia a fin de obtener aplicaciones de mainframe modernas.

Según el estudio de Forrester Consulting solicitado por BMC en 2021 Modernizing Mainframe Development Tools Can Help Drive Greater ROI, más de tres cuartas partes de los desarrolladores consideran que el mainframe tiene una importancia vital para su empresa. Sin embargo, ocho de cada diez manifestaron que sus herramientas de desarrollo de mainframe requieren mejoras sustanciales para ser más útiles. El estudio concluyó que los equipos con herramientas modernas consiguen crear aplicaciones de mainframe modernas y encuentran menos problemas en cuanto a la falta de competencias y la adquisición de los mejores talentos.

Ahora, la solución BMC Compuware ISPW se integra con GitHubActions y HCL Launch para automatizar el desarrollo de aplicaciones de mainframe y el proceso de despliegue, reduciendo el coste y la complejidad.

GitHub Actions y HCL Launch amplían las integraciones CI/CD actuales en la solución BMC Compuware ISPW. Estas incluyen Jenkins, Git, GitLab, GitHub, VS Code y API REST. Con GitHub Actions, los usuarios limitan los errores y aumentan la calidad de la aplicación estableciendo canales de CI/CD con flujos de trabajo automatizados.

Gracias a HCL Launch, los desarrolladores coordinan despliegues automatizados desde múltiples entornos con un solo clic. Además, HCL Launch amplía las integraciones de CD vigentes desde BMC con Digital.ai Release y CloudBees Flow para lograr despliegues más rápidos y fáciles.

En la actualidad, los clientes pueden utilizar un plugin HCL Launch para la solución BMC AMI DevOps for Db2 para capturar y propagar de forma automática las modificaciones de las bases de datos en entornos Db2®, así como en Jenkins e IBM® UrbanCode® Deploy.

Identificar rápidamente problemas de funcionamiento con Java

La solución AMI Ops Monitor de BMC para Java Environments descubre automáticamente todas las máquinas virtuales Java (JVM) en z/OS®. De este modo, los usuarios pueden detectar y reparar problemas rápidamente, identificando los problemas de funcionamiento causados por JVM y conociendo sus repercusiones en otros flujos de trabajo. Estas prestaciones nuevas y ampliadas garantizan una mayor disponibilidad y un tiempo de respuesta más breve porque permiten que el mainframe realice acciones de diagnóstico y vea la información sobre las API y los servicios que utilizan las JVM.

BMC se une al proyecto de mainframe abierto Zowe
La nueva herramienta Workflow WiZard de BMC ha sido aceptada como parte del marco Zowe, proyecto de código abierto integrado y extensible para z/OS. Workflow WiZard facilita el trabajo de desarrolladores y sistemas optimizando la instalación, la configuración y el mantenimiento del software IBM z/OS y de los productos informáticos de otros distribuidores de software independientes. Esta contribución pone de relieve el compromiso de la compañía con Open Mainframe Project y representa una gran oportunidad para colaborar con la comunidad mainframe e incrementar la innovación en la plataforma z/OS.

“Los clientes confían en BMC para la transformación de su mainframe. En BMC bloqueamos las amenazas internas al mainframe, aumentamos la entrega, la calidad, la velocidad y la eficiencia de software y reforzamos la resiliencia operativa”, afirma John McKenny, vicepresidente ejecutivo y director general de Intelligent Z Optimization and Transformation en BMC. "Con estas prestaciones nuevas y ampliadas para nuestras soluciones BMC AMI y BMC Compuware, pueden seguir convirtiendo el mainframe en un polo de innovación para cualquier Autonomous Digital Entreprise.”

[1]“Best Practices: Mitigating Insider Threat”, Forrester, 18 de marzo de 2021

Otros recursos

Conocer las novedades sobre soluciones BMC de mainframe.
Seguir leyendo sobre la seguridad, la innovación y la colaboración que conducen a la transformación del mainframe.
Descubrir cómo llegar a ser una Autonomous Digital Entreprise.

Acerca de BMC
BMC ofrece software básico, servicios cloud e innovación que permite a más de 10.000 clientes de todo el mundo (incluido el 84% del Forbes Global 100) evolucionar hasta convertirse en una Autonomous Digital Entreprise.

Datos de contacto:
Círculo de Comunicación
910 001 948

Nota de prensa publicada en: Madrid

Categorías: Programación E-Commerce Software Ciberseguridad