RSA® ARCHER® CONTINUOUS MONITORING

Caso de uso para soluciones del sector público

El reto

Los controles de seguridad no se evalúan con suficiente frecuencia. Las evaluaciones se realizan con herramientas de diferentes proveedores, con formatos de datos de propiedad y uso compartido de datos limitado. Se obtienen más resultados de los que el personal disponible puede administrar. La corrección de los resultados no tiene un orden de prioridad en función de todos los datos contextuales disponibles. El monitoreo continuo (CM) es una combinación de evaluaciones manuales y automatizadas. Los proveedores que producen herramientas automatizadas de análisis o sensores comercializan su producto como "soluciones de monitoreo continuo". Sin embargo, no proporcionan evaluaciones manuales, y la mayoría solo evalúa un tipo de falla (vulnerabilidad o configuración incorrecta), mientras que la orientación sobre CM del NIST (Instituto Nacional de Normas y Tecnología) y el DHS (Departamento de Seguridad Nacional de los Estados Unidos) define varios tipos de fallas. Las actualizaciones de FISMA (Ley Federal de Administración de la Seguridad de la Información) y la orientación reciente de la OMB (Oficina de Administración y Presupuesto) presionan a las organizaciones para avanzar con su planificación de CM, pero la falta de antecedentes crea incertidumbre a la hora de considerar los detalles de implementación más específicos.

Hasta este momento, la falta de CM en la comunidad de agencias federales implicaba que las fallas y las vulnerabilidades permanecían sin corrección por largos períodos. También es difícil compartir los datos o crear una imagen general del riesgo debido a las discrepancias entre las herramientas y los resultados de las evaluaciones incompletos o desactualizados. No hay personal suficiente para realizar todas las evaluaciones y corregir todos los resultados. La falta de contexto y visibilidad implica que las fallas más importantes no siempre se corrigen primero. Por ejemplo, ¿debe corregirse primero un resultado importante en un sistema moderado o un resultado moderado en un sistema importante? La mayoría de las organizaciones no tienen la información ni las métricas para realizar una clasificación de las fallas, en especial, teniendo en cuenta la criticidad del sistema de información.

Descripción general

RSA® Archer® Continuous Monitoring funciona como un hub para varios tipos de análisis y sensores, lo que permite a la organización crear una vista agregada de riesgos en todos los niveles de la empresa. En el extremo inferior, las fallas individuales se pueden monitorear y puntuar. Las fallas se agregan en cada nivel de la jerarquía, desde el nivel de dispositivos individuales hasta el nivel de departamentos. De esta manera, se puede designar un puntaje de riesgo en cualquier capa y se puede medir la cantidad de riesgo relativo que se introduce. Esto permite que los recursos limitados se enfoquen en las iniciativas de corrección que proporcionarán el mayor beneficio.

Con RSA Archer Continuous Monitoring, puede brindar una respuesta más rápida y más dirigida a los riesgos que surgen. Su personal será capaz de moderar los resultados en el orden que permita reducir más los riesgos. Cuando se usa en conjunto con RSA Archer Assessment and Authorization, puede mejorar las actividades de cumplimiento de normas de FISMA y de OMB verificando que los sistemas de información respeten los acuerdos de autorización (ATO o autorización para operar) y que funcionen dentro de los niveles aceptables de riesgo. Esto genera

un ambiente más seguro con más información valiosa y la capacidad de tomar decisiones sobre riesgo mejores y más informadas.

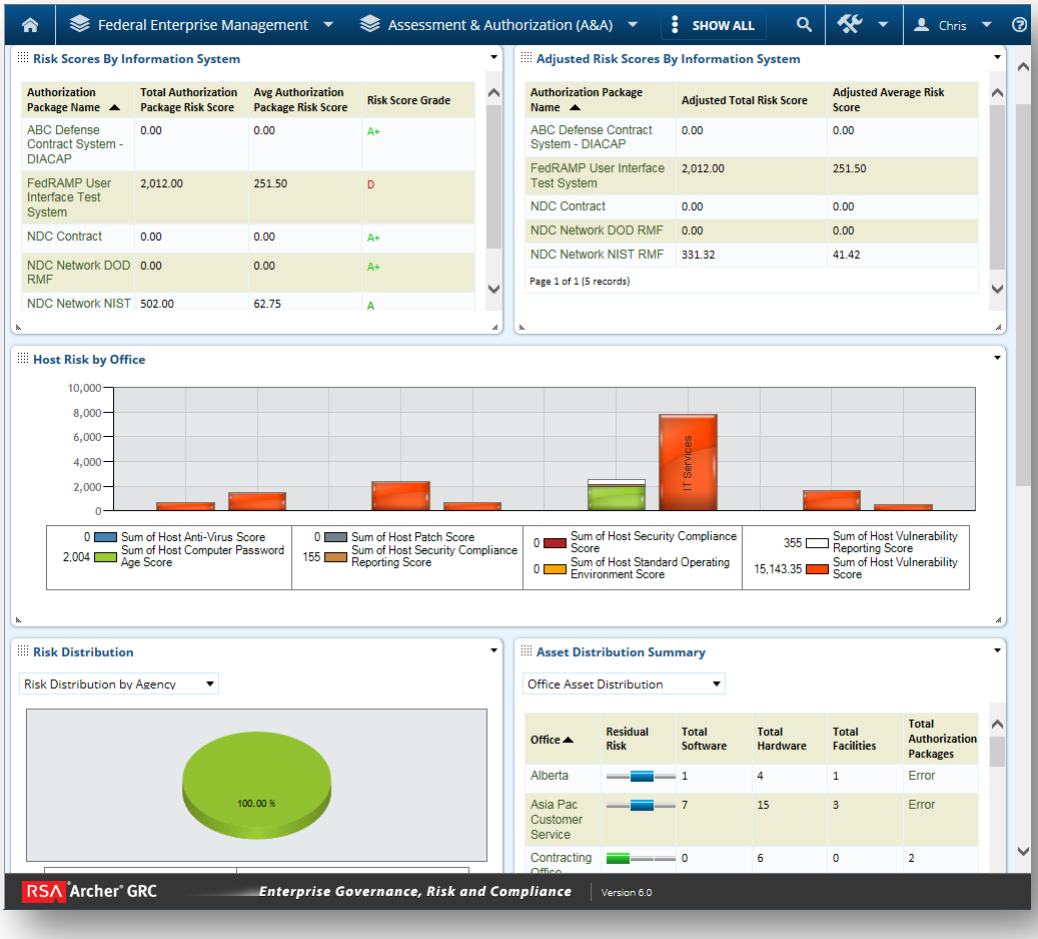
Funciones clave

- Inventarios de hardware y software actuales y autorizados
- Bibliotecas de fallas actuales
- Integración de los análisis y los sensores en un ambiente común, con un formato común
- Algoritmos de puntuación y clasificación para cada falla, dispositivo y capa de la jerarquía organizacional
- Rastreo y corrección de las fallas

Beneficios clave

RSA Archer Continuous Monitoring proporciona:

- Reducción del tiempo de exposición
- Reducción del riesgo general
- Aumento de la visibilidad y mejor toma de decisiones
- Datos de riesgo más actuales
- Aumento de la seguridad (confianza basada en los datos actuales)



Para obtener más información

Para obtener más información acerca de cómo los productos, los servicios y las soluciones de EMC pueden ayudarlo a superar sus retos de TI y del negocio, comuníquese con su representante local o con un reseller autorizado, o visítenos en www.rsa.com. Si ya es cliente de RSA Archer y tiene preguntas o necesita información adicional sobre licencias, comuníquese con RSA Archer mediante archersupport@rsa.com o llame al +52-55-5080-3700.

RSA
www.rsa.com