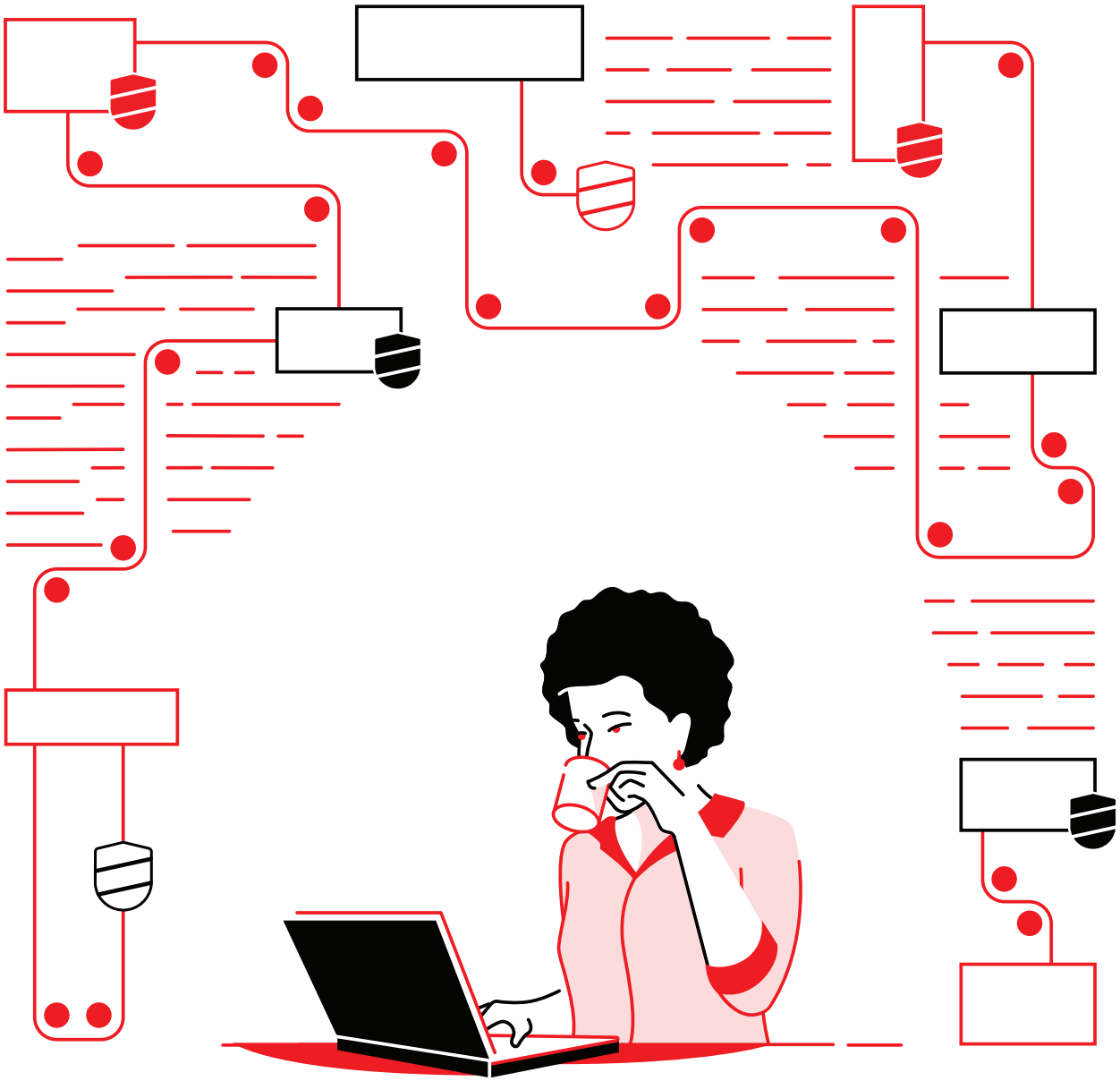
Simplifique su centro de operaciones de seguridad

Obtenga más velocidad, tiempo y seguridad con una plataforma de automatización unificada



Red Hat | IBM

Conozca el contenido

La seguridad de la TI es uno de los principales temas de interés de las empresas

Para la mayoría de las empresas, la seguridad es uno de los temas más importantes. De hecho, el 33 % de los directores ejecutivos expresó una gran preocupación por las amenazas cibernéticas[1]. Y no se trata de un temor infundado, ya que el 32 % de las empresas sufrió ciberataques graves durante los últimos dos años[2].

Proteger su empresa es una tarea fundamental, pero en ocasiones es abrumadora. Los equipos de seguridad deben ensamblar, mantener, gestionar y adaptar los entornos complejos utilizando varios servicios y herramientas de distintos proveedores que compiten unos con otros. Cada año hay más ofertas, así que los equipos deben investigar, evaluar e integrar los productos nuevos permanentemente, a medida que cambia el panorama de la seguridad.

Además, las fallas siguen aumentando en cantidad, gravedad y costo. La probabilidad de sufrir una filtración de datos en un plazo de dos años es del 29,6 %, frente al 22,6 % que se reportó en el 2014[3]. La cantidad promedio de registros involucrados en cada una de ellas aumentó un 3,9 % entre el 2018 y el 2019[3], mientras que su costo promedio alcanzó los US$ 3,92 millones en el 2019[3].

La mayoría de las empresas gestionan las operaciones de seguridad de forma manual. La intervención de las personas hace que estas tareas lleven mucho tiempo y se vuelvan tediosas y propensas a errores. En consecuencia, los equipos de seguridad suelen sentirse abrumados, ya que deben abordar una cantidad cada vez mayor de alertas por amenazas que envían las diversas herramientas. De hecho, el 60 % de ellos recibe más de 5000 alertas por día, mientras que un 16 % recibe más de 100 000[4].

El aumento del tamaño y la complejidad de la infraestructura solo dificultaría más la identificación de los puntos vulnerables y la verificación de las filtraciones de datos. Como la mayoría de las herramientas de seguridad no se integran entre sí, el personal encargado de la seguridad debe realizar más tareas manuales, lo que incrementa los tiempos de investigación y resolución de incidentes. En el 2019, el tiempo promedio para identificar y contener una filtración de datos fue de 279 días, lo cual representa un aumento del 4,9 % respecto del 2018[3]. Además, el 39 % de las empresas informó una escasez de personas capacitadas en materia de ciberseguridad en el 2019, lo cual demuestra que es difícil encontrar al personal adecuado para ampliar los equipos y mantenerse actualizado[2]. Por último, los presupuestos que se destinan a la ciberseguridad son limitados: solo el 33 % de las empresas cuenta con fondos suficientes para obtener un nivel alto de seguridad informática[5].

Esto genera que los equipos de seguridad tradicionales solo analicen y aborden el 48 % de las alertas que reciben y que solucionen únicamente el 50 % de las amenazas legítimas[4], así que muchas empresas quedan vulnerables a sufrir ataques.

El 77 % de las empresas tiene pensado aumentar la automatización para simplificar y acelerar los tiempos de respuesta en sus ecosistemas de seguridad[4].

Efectos de la falta de eficacia en materia de seguridad

Las fallas de seguridad siguen aumentando en cantidad, gravedad y costo.

US$ 3,92 millones:
costo promedio de una filtración de datos en el 2019[3]

279 días:
tiempo promedio para identificar y contener una filtración de datos en el 2019[3]

US$ 1,22 millones:
ahorro en costos si se detecta y detiene una filtración en **200 días** o menos[3]

29,6 %:
probabilidad de sufrir una filtración de datos en un período de dos años[3]

50 %:
proporción de amenazas legítimas que se solucionan[4]

1 *PWC, "23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty", 2020.* pwc.com/ceosurvey.

2 *Harvey Nash y KPMG, "CIO Survey 2019: A Changing Perspective", 2019.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.

3 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.

4 *Cisco, "Cisco Benchmark Study: Securing What's Now and What's Next", febrero de 2020.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.

5 *Ponemon Institute, patrocinado por IBM Security, "The Cyber Resilient Organization", abril del 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

¿Qué es la automatización de la seguridad?

Es un procedimiento que consiste en automatizar las tareas manuales relacionadas con el mantenimiento de la estrategia de seguridad de su empresa. Se trata de una serie de prácticas que dividimos en cuatro categorías generales:

Respuesta y corrección
Actividades basadas en eventos que implican la participación y la orientación de los analistas de seguridad

Operaciones de seguridad
Actividades diarias basadas en políticas y procesos que los equipos de tecnología llevan a cabo en su infraestructura de seguridad

Cumplimiento de la seguridad
Actividades destinadas a garantizar el cumplimiento de la infraestructura con las políticas y las normas de seguridad

Fortalecimiento
Tareas para aplicar políticas de seguridad personalizadas en la infraestructura con intenciones y objetivos determinados

Obtenga más información sobre el cumplimiento y el fortalecimiento de la seguridad

Lea estos recursos y descubra cómo la automatización le permite cumplir con las normas de seguridad y reforzarla:

- Ebook: Aumente la seguridad de la nube híbrida
- Whitepaper: Automatización de la seguridad y el cumplimiento gracias a Red Hat
- Datasheet: Servicios de Red Hat: Automatización de los flujos de trabajo de confiabilidad y seguridad

Este ebook se centra en la automatización de las operaciones de seguridad y las tareas de respuesta y corrección.

Beneficios de la automatización para las operaciones de seguridad y las actividades de respuesta y corrección

Aumente la rapidez y la eficiencia

La automatización optimiza las tareas y elimina la necesidad de intervenir manualmente, lo cual agiliza las operaciones de seguridad y permite que el personal vuelva a concentrarse en las iniciativas de gran valor. Además, reduce la complejidad de la infraestructura de TI: el 40 % de las empresas con un gran nivel de automatización afirma tener la cantidad adecuada de soluciones y tecnologías de seguridad[6].

Mejore la seguridad a escala

Si automatiza toda su infraestructura de seguridad, podrá aumentar la uniformidad y adoptar un enfoque más integral. Como cada miembro del personal gestiona más herramientas, dispositivos y sistemas, usted puede ajustar sus operaciones según sea necesario. La automatización también reduce el riesgo de que se cometan errores humanos y, de esta manera, mejora la precisión.

Reduzca el riesgo y el costo de las filtraciones de datos

Las empresas con un alto nivel de automatización pueden evitar más los fallos de seguridad y las interrupciones de las actividades comerciales[6]. Si automatiza todo el sistema de seguridad, puede reducir en un 95 % el costo promedio de una filtración de datos[7]. Por eso, el 52 % de las empresas ya la implementó en cierto nivel, y otro 36 % más planea hacerlo en los próximos 24 meses[7].

6 *Ponemon Institute, patrocinado por IBM Security, "The Cyber Resilient Organization", abril del 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

7 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.

La automatización integra sus procesos, sistemas y herramientas de seguridad

Utilice una plataforma flexible y uniforme para unir a las personas, los procesos y las herramientas

Una plataforma de automatización puede posibilitar la integración entre sus equipos, herramientas y procesos de seguridad. Si es flexible e interoperable, podrá:

- Conectar sus sistemas, herramientas y equipos de seguridad.
- Recopilar información de los sistemas y enviarla a las ubicaciones y los sistemas predefinidos con rapidez y sin intervención manual.
- Cambiar y propagar configuraciones rápidamente desde interfaces centralizadas.
- Crear y mantener el contenido de automatización personalizado que se relaciona con sus herramientas y procesos de seguridad, y acceder a él.
- Activar acciones automatizadas en múltiples herramientas de seguridad cuando se detecta una amenaza.

El uso de un lenguaje y una plataforma de automatización uniformes en toda la empresa le permite mejorar la comunicación y la colaboración. Si se utiliza el mismo lenguaje para automatizar todas las soluciones de una cartera de productos de seguridad, los analistas y los operadores pueden realizar múltiples tareas en distintos productos en mucho menos tiempo, lo cual aumenta al máximo la eficiencia general del equipo de seguridad. Asimismo, tener un marco y un lenguaje comunes permite que los equipos de seguridad y TI compartan diseños, procesos e ideas con mayor facilidad, tanto con los demás miembros del equipo como con el resto de la empresa.

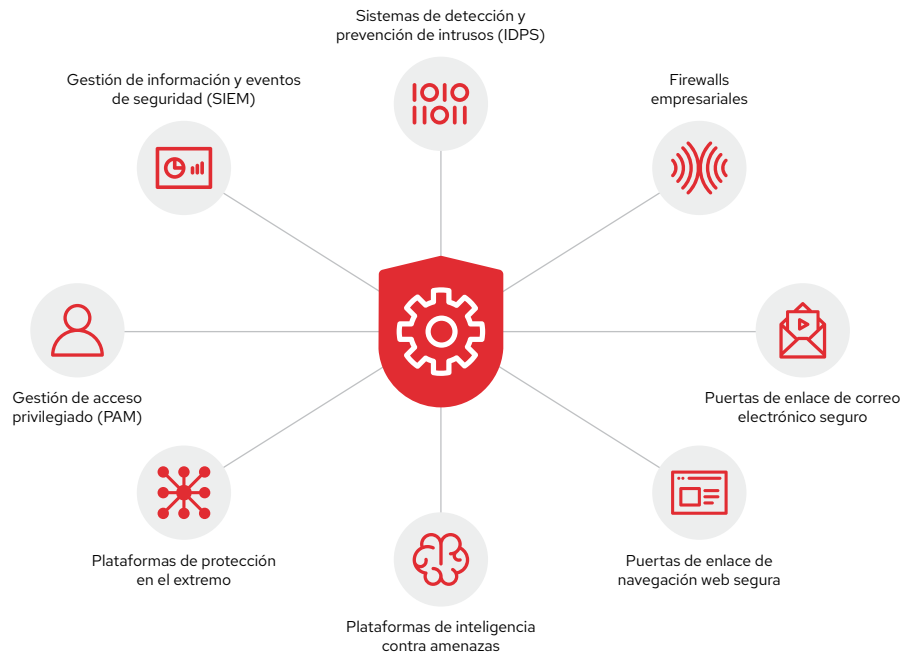


Figura 1. Una plataforma de automatización puede conectar sus sistemas, herramientas y equipos de seguridad.

Éxito de la automatización = capital humano + procesos + plataformas

Para aprovechar al máximo el valor de la automatización no solo necesita una herramienta; también debe tener en cuenta a las personas, los procesos y las plataformas.

- **Las personas** son la parte más importante de las iniciativas empresariales. La participación dentro del equipo y con el resto de la empresa permite colaborar y compartir ideas con mayor facilidad.
- **Los procesos** permiten que los proyectos avancen por las distintas etapas en su empresa, desde el inicio hasta la finalización. Si quiere lograr una automatización eficiente, deben ser claros y estar documentados.
- Una **plataforma** de automatización proporciona las funciones necesarias para diseñar, ejecutar y gestionar los recursos para implementarla. A diferencia de las herramientas de automatización sencillas, esta plataforma ofrece a su empresa una base unificada para crear proyectos de este tipo, implementarlos y compartir conocimiento y contenido coherentes sobre la automatización según sea necesario.

Leer el ebook

La automatización de la seguridad es un proceso

Su implementación en algún ámbito de la empresa no es algo que sucede de la noche a la mañana, ni tampoco en un solo paso. Es más bien un proceso. Cada empresa decide en qué momento implementarla o dejar de hacerlo según sus necesidades, las cuales también determinan qué camino debe tomar. De todas formas, no importa en qué punto de la adopción se encuentre, ya que incluso las pequeñas iniciativas de automatización de la seguridad pueden resultar benéficas.

Evalúe el nivel de consolidación de la automatización de la seguridad

La mayoría de las empresas están en una de las tres etapas principales de consolidación de la automatización de la seguridad. Determinar en cuál se encuentra le permitirá adoptar las herramientas y los procesos adecuados en el momento oportuno, y así implementar la automatización con éxito.

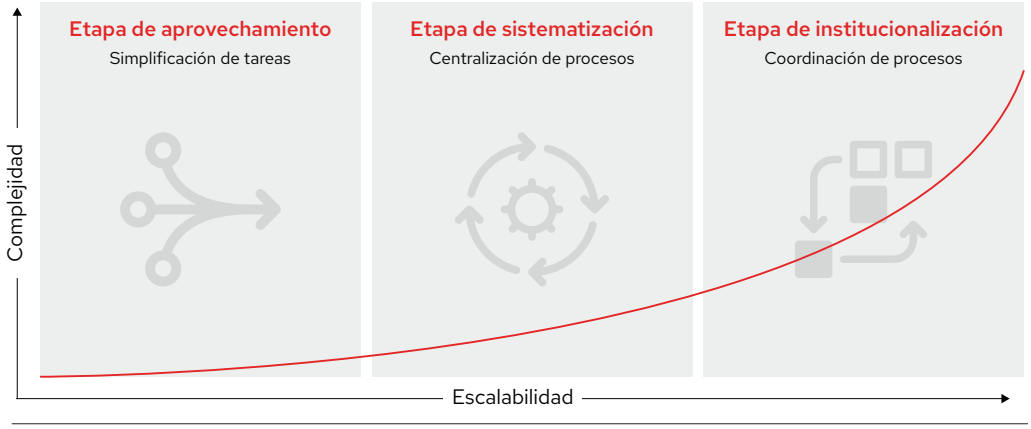


Figura 2. *Etapas para consolidar la automatización de la seguridad*

Etapa 1: Aprovechamiento

Esta etapa se enfoca en ahorrar tiempo mediante la automatización de las tareas de seguridad. Entre los objetivos comunes se encuentran estandarizar las operaciones de seguridad en los dispositivos y las tecnologías similares, y simplificar las tareas manuales que se realizan en los productos de diferentes proveedores.

Etapa 2: Sistematización

Esta etapa se centra en mejorar los procesos y la eficiencia mediante la adopción de un conjunto uniforme de herramientas y servicios para llevar a cabo las operaciones de seguridad. Entre los objetivos comunes se encuentran diseñar procesos de seguridad en los flujos de trabajo superiores y centralizar los procesos de respuesta.

Etapa 3: Institucionalización

Esta etapa se enfoca en impulsar la colaboración e integrar la seguridad a toda la empresa. Entre los objetivos comunes se encuentran crear flujos de trabajo programáticos y automatizados que abarquen todos los aspectos de la seguridad, e integrar sus tecnologías de TI y seguridad.

Defina su camino hacia la automatización de la seguridad

Casos de uso comunes y de gran importancia para la automatización de la seguridad

Cada uno de ellos puede servirle como punto de partida. La clave es comenzar poco a poco y crecer con el tiempo.

Enriquecimiento de la investigación

Cuando se investigan las alertas y los incidentes, se recopila información de los diversos sistemas de seguridad para evaluar si se produjo un evento legítimo. Normalmente, se lleva cabo a través de las interfaces de usuario, los correos electrónicos y las llamadas telefónicas. Este proceso ineficiente puede retrasar las acciones que se deban tomar contra las amenazas, lo cual deja puntos vulnerables en su empresa y aumenta los posibles costos asociados a una filtración de datos. Con la automatización, puede recopilar información de manera programática en sus sistemas de seguridad, lo cual respalda el enriquecimiento de las evaluaciones que se realizan por medio de un sistema de gestión de información y eventos de seguridad (SIEM), cuando lo solicite. Esto le permitirá analizar las alertas y los incidentes, y abordarlos con mayor rapidez.

Búsqueda de amenazas

Este caso de uso implica identificar e investigar las posibles amenazas a la seguridad de manera anticipada. Al igual que ocurre en la investigación de incidentes, el personal recopila y envía información de un sistema a otro manualmente. Con la automatización, puede personalizar y optimizar las alertas, las búsquedas de correlación y la administración de firmas, para evaluar las posibles amenazas en menos tiempo. También le permite crear y actualizar automáticamente las consultas de correlación de SIEM y las reglas del sistema de detección de intrusos (IDS). Como resultado, podrá actualizar la protección de su empresa de forma más frecuente y con mayor eficiencia.

Respuesta ante los incidentes

Esto implica tomar medidas para detener una filtración de datos. Una vez detectada, el personal de seguridad debe responder con rapidez y a escala para controlarla. Sin embargo, las acciones de respuesta suelen incluir varias tareas manuales, lo cual retrasa el tiempo de corrección y deja vulnerable a la empresa por más tiempo. La automatización codifica estas acciones en playbooks repetibles y aprobados previamente, para que pueda solucionar los problemas con mayor rapidez. Además, le permite agilizar ciertas tareas, como bloquear las direcciones IP o los dominios desde donde se realizan los ataques, permitir el tráfico seguro, congelar las credenciales comprometidas y aislar las cargas de trabajo sospechosas, de modo que pueda investigarlos y minimizar los daños asociados con el incidente.

La integración es fundamental

Si desea aplicar un enfoque unificado, necesita integrar su plataforma de automatización y sus tecnologías de seguridad. Las integraciones fundamentales abarcan:

- **Firewalls:** controlan el flujo de tráfico entre las redes y protegen las aplicaciones que están expuestas a Internet. La automatización agiliza los cambios en la configuración de las políticas y los registros.
- **Sistemas de detección y prevención de intrusos (IDPS):** supervisan el tráfico de red en busca de actividades sospechosas, emiten alertas de amenazas y bloquean los ataques. La automatización simplifica la gestión de las normas y los registros.
- **Sistemas de gestión de información y eventos de seguridad:** recopilan y analizan los eventos de seguridad para detectar las amenazas y responder a ellas. La automatización le brinda acceso a las fuentes de datos mediante programación.
- **Herramientas de gestión de acceso privilegiado (PAM):** supervisan y gestionan las cuentas y los accesos que tienen privilegios. La automatización optimiza la gestión de las credenciales.
- **Sistemas de protección en el extremo:** supervisan y administran los dispositivos para mejorar su seguridad. La automatización simplifica las tareas comunes de este tipo de gestión.

Simplifique el centro de operaciones de seguridad con Red Hat Ansible Automation Platform

Si bien hay muchas soluciones de automatización disponibles, no todas incluyen las funciones necesarias para automatizar la seguridad de manera eficiente. Busque plataformas de automatización que ofrezcan:

- **Un lenguaje de automatización universal y accesible.** Debe poder entenderse y escribirse con facilidad. Esto le permitirá documentar y compartir información con los miembros del equipo de seguridad que tienen experiencia en otros dominios.
- **Un enfoque abierto y objetivo.** Para ser eficiente, la plataforma de automatización debe interactuar con todo el ecosistema del proveedor y la infraestructura de seguridad.
- **Un diseño ampliable y en módulos.** Las plataformas modulares permiten implementar la automatización en etapas, mientras que la extensibilidad lo ayuda a adaptar las herramientas de seguridad adicionales y futuras de otros proveedores cuando lo necesita.

Impulse a su equipo de seguridad con Red Hat

Red Hat® Ansible® Automation Platform constituye una base para diseñar y ejecutar servicios de automatización a escala, y ofrece las herramientas y las funciones necesarias para implementar la automatización de la seguridad. Combina un lenguaje sencillo y fácil de leer con un entorno de ejecución confiable y acoplable, y funciones de colaboración y uso compartido centradas en la seguridad. Con una base abierta, puede conectar y automatizar prácticamente todos los aspectos de su infraestructura de seguridad y TI, lo que da lugar a una plataforma común que propicia la participación y la colaboración en toda la empresa. Red Hat Ansible Automation Platform también ha generado resultados comprobados en otras áreas, como las operaciones de TI y de red y DevOps.

Incluye un conjunto de **colecciones de Ansible centradas en la seguridad** que ofrecen módulos, funciones y playbooks. Estos recursos coordinan la actividad de varias clases de soluciones de seguridad para brindar una respuesta más unificada a las amenazas cibernéticas y las tareas de seguridad, lo que abarca:

- Unir los flujos de trabajo y los playbooks para poder reutilizarlos en forma modular.
- Consolidar y centralizar los registros.
- Admitir los controles de acceso y los servicios del directorio local.
- Integrar las aplicaciones externas usando las interfaces de programación de aplicaciones (API) de REST.

Red Hat Ansible Automation Platform también incluye herramientas y funciones para que pueda optimizar la automatización. **Automation Analytics** brinda información relevante sobre cómo su empresa utiliza la automatización. **Automation Hub** permite que los miembros del equipo accedan al contenido certificado mediante un repositorio centralizado. Y **Content Collections** optimiza la gestión, la distribución y la utilización de los recursos de automatización.

Obtenga ayuda de los especialistas

Red Hat puede ayudarlo a implementar la automatización con mayor rapidez.

- **Red Hat Services Program: Automation Adoption** ofrece un marco para gestionar el proceso de adopción en toda la empresa.
- **Red Hat Training and Certification** ofrece certificaciones y cursos de capacitación prácticos para que pueda usar la automatización de forma más eficiente.
- El **Soporte de Red Hat** trabaja con usted para garantizar el éxito de su TI. Ofrecemos un soporte web galardonado[8] que le permite acceder a prácticas recomendadas, documentación, actualizaciones y alertas y parches de seguridad. También puede ponerse en contacto con un ingeniero de soporte o con un gerente de cuentas técnicas para resolver sus problemas y obtener orientación especializada.
- Las **colecciones certificadas de contenido para partners** le permiten automatizar fácilmente el hardware y el software de múltiples proveedores. Este contenido de automatización confiable y prediseñado está disponible a través de Automation Hub, y cuenta con el respaldo tanto del partner como de Red Hat.

8 Premios y reconocimientos, Portal de clientes Red Hat.

La automatización en acción

Red Hat Ansible Automation Platform ofrece valor empresarial comprobado

Esta plataforma le permite automatizar su centro de operaciones de seguridad de manera más eficiente y optimizada. Los informes de los analistas de las empresas que utilizan Red Hat Ansible Automation Platform demuestran un valor comercial medible. De hecho, miembros del **IDC** entrevistaron a varios responsables de la toma de decisiones sobre sus experiencias con dicha plataforma, y llegaron a la conclusión de que cada empresa obtuvo beneficios importantes en materia de productividad, agilidad y operatividad gracias a la automatización.

más eficiencia y productividad por parte de los equipos de seguridad de la TI[9]

más eficiencia en la reducción de fallos de seguridad[9]

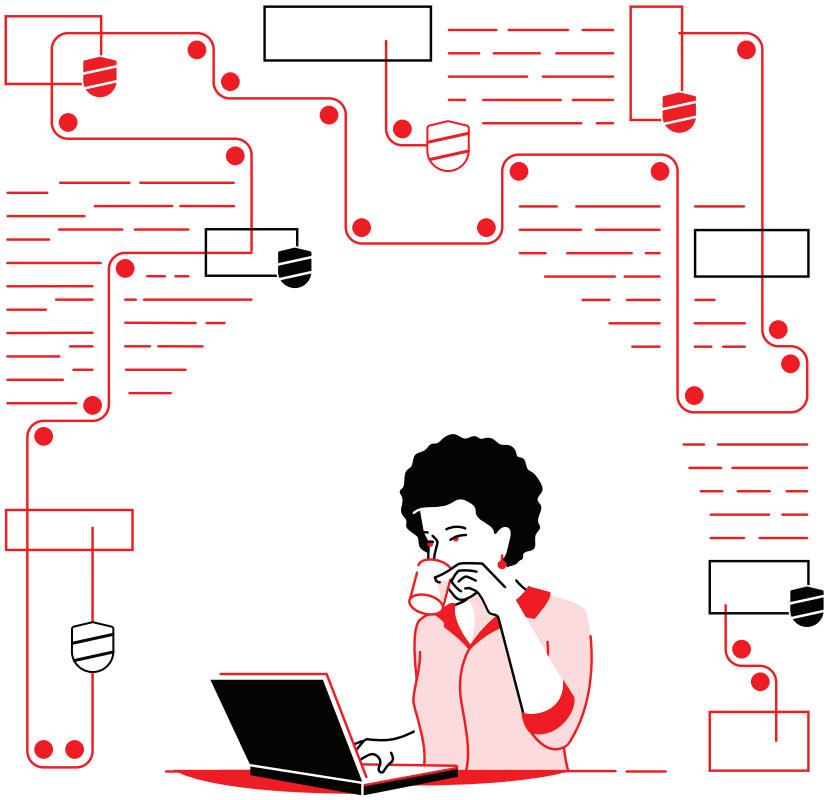
más eficiencia en la aplicación de parches de seguridad[9]

"Red Hat Ansible [Automation Platform] es la opción ideal para unir a nuestros equipos de TI. Los equipos del servidor, la seguridad, la red y la base de datos pueden trabajar en sus respectivos niveles, y luego usar Red Hat Ansible Automation para crear sus propios playbooks".[9]

9 Whitepaper de IDC, patrocinado por Red Hat. "Red Hat Ansible Automation mejora la agilidad de la TI y acelera la comercialización", junio del 2019.

¿Está listo para simplificar su centro de operaciones de seguridad?

La automatización puede ayudarlo a identificar y responder a las crecientes amenazas de seguridad de manera más rápida y a escala. Red Hat le ayuda a proteger su empresa conectando sus equipos, herramientas y procesos de seguridad con una plataforma de automatización colaborativa y coherente.



Aprenda a automatizar la seguridad con Red Hat Ansible Automation Platform

F24343_0720_KVM

Red Hat | IBM