Red Hat

Mejor seguridad gracias a la automatización

Una serie de casos de éxito de los clientes de Red Hat

Contenido

Introducción

La automatización perfecciona la seguridad

El desafío de integrar los equipos y las soluciones de seguridad de la TI en un entorno dinámico es un requisito que toda empresa debe cumplir. Si bien cada enfoque hacia la seguridad es diferente, es posible aprender y adaptar ciertas estrategias para proteger las aplicaciones, los sistemas de TI, las redes, los dispositivos y los datos valiosos de actividades maliciosas o no deseadas.

En este ebook queremos compartir estas estrategias, por lo que destacamos cinco casos de éxito de clientes de Red Hat® Ansible® Automation Platform que usan la automatización para integrar y expandir las soluciones de seguridad con el fin de investigar las amenazas y responder a ellas en toda la empresa de manera coordinada y unificada.

La automatización mejora la seguridad

La mayoría de las empresas cuenta con un equipo de seguridad que sabe lo que debe hacer. Sin embargo, configurar manualmente los sistemas y las aplicaciones para protegerse de los ataques toma más tiempo y recursos especializados de lo que resulta práctico, en especial cuando estos sistemas y aplicaciones son miles.

La automatización permite hacer frente a la falta de personal y recursos capacitados al aplicar y hacer cumplir estándares de seguridad que se adaptan para cumplir las directrices internas y externas de seguridad. Los resultados son la reducción drástica de los tiempos de respuesta y la disminución de los puntos vulnerables.

> ***Las empresas que cuentan con IA y automatización de la seguridad completamente implementadas pudieron detectar y contener las fallas mucho más rápido que las empresas sin esta ventaja.***
>
> IBM. "Cost of a Data Breach Report 2022", julio de 2022.

Ansible Automation Platform ayuda a los equipos a automatizar e integrar soluciones de seguridad que permiten investigar las amenazas y responder a ellas en toda la empresa de manera coordinada y unificada, mediante un conjunto organizado de módulos, funciones y playbooks.

¿Qué incluye un enfoque unificado hacia la seguridad?

Las soluciones de seguridad están en evolución constante para mantenerse un paso adelante de las amenazas. Algunos de los aspectos que se deben considerar son los siguientes:

Enriquecimiento de la investigación

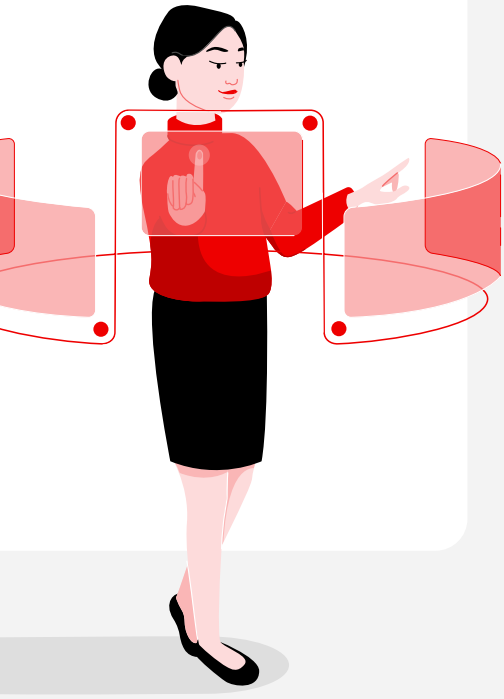
La recopilación de los registros de todos los firewalls, los sistemas de detección de intrusiones (IDS) y otros sistemas de seguridad permiten enriquecer de manera programática y según sea necesario las actividades de evaluación que se realizan mediante la gestión de la información y los eventos de seguridad (SIEM).

Búsqueda de amenazas

Configure el nivel de registros automáticamente, y cree reglas nuevas para los IDS y políticas nuevas para los firewalls con el fin de facilitar la detección de más amenazas en menos tiempo.

Respuesta ante los incidentes

Corrija errores más rápidamente con acciones automatizadas, como la elaboración de listas negras de dominios o direcciones IP, la elaboración de listas blancas de tráfico seguro o el aislamiento de cargas de trabajo sospechosas para su investigación.



Ventajas de elegir Ansible para automatizar la seguridad

La seguridad es responsabilidad de todos. Ansible es una herramienta potente y sin agentes que permite que la automatización sea accesible en toda la empresa, desde los equipos de operaciones de TI, los de desarrollo y los de ingeniería de redes hasta los equipos de seguridad, ya que la ofrece en un lenguaje que las personas pueden comprender. Esto posibilita que las empresas saquen más provecho de la automatización y:

- Aumenten la productividad. Ansible usa un lenguaje simple que las personas pueden comprender, por lo que no se necesitan habilidades especializadas de codificación o gestión para asegurar que las tareas se ejecuten en el orden adecuado.
- Gestionen toda la infraestructura de TI. Obtienen la habilidad de reunir y auditar información, además de mantenerse actualizadas en cuanto a la gestión y la organización de los flujos de trabajo.
- Aumenten la efectividad y la seguridad. La arquitectura sin agentes le permite implementar soluciones con más rapidez sin los aspectos vulnerables de los agentes para explotar o actualizar.

Los casos de éxito siguientes ilustran la potencia y la capacidad de ajuste de la automatización para la seguridad, y la manera en que una plataforma unificada de automatización, como Ansible Automation Platform, ayuda a las empresas a mejorar su postura en cuanto a la seguridad.

1

EMORY UNIVERSITY

Emory University reduce las amenazas de sudo con Red Hat Ansible Automation Platform

> *No pensaban que pudiéramos aplicar parches a los servidores de Linux cada 30 días, pero con Red Hat Ansible Automation Platform no solo es posible, sino necesario.*
>
> Steve Siegelman, gerente de ingeniería en sistemas, Oficina de Tecnología de la Información, Emory University

Emory University se ubica en Atlanta, Georgia y aloja a más de 15 000 estudiantes en los campus del área metropolitana de Atlanta. Esta institución tiene vínculos de investigación en todo el mundo y opera el sistema de atención médica más grande de Georgia, por lo que es natural que sea el objetivo de ataques cibernéticos que buscan obtener acceso a la información confidencial mediante su entorno digital.

Una vez que un punto vulnerable permite una entrada, la preocupación está en que el atacante podría moverse de manera clandestina en toda la red, tomar elementos de propiedad intelectual y escapar sin ser detectado. La Oficina de Tecnología de la Información (OIT) de la universidad debe mantener los sistemas para los estudiantes, el personal, los profesores, los investigadores y las demás partes interesadas para garantizar que las redes y los datos estén protegidos de los accesos no autorizados y los posibles fallos de seguridad. Por este motivo existió tanta preocupación cuando, en enero de 2021, el equipo de Red Hat alertó a la OIT de un punto vulnerable dentro de los sistemas de Red Hat Enterprise Linux® de Emory, el cual afectaba la herramienta de sudo del sistema operativo.

La automatización con Ansible agiliza la resolución de riesgos de seguridad

Aplicación de parches en horas en lugar de semanas

La OIT, que tiene más de 500 servidores que usan Red Hat Enterprise Linux a su cargo, sabía que tenían un camino difícil por delante si debían instalar el parche manualmente, lo cual habría puesto a la infraestructura de la universidad en peligro. La solución fue usar un playbook de Ansible para aplicar los parches a cada servidor de manera automática. Lo que hubiera tomado hasta dos semanas en solucionarse en todos los servidores tomó, en total, cuatro horas.

Los recursos humanos valiosos cuentan con más tiempo para centrarse en los proyectos importantes

Ansible Automation Platform se usó en principio en los sistemas financieros de Emory antes de que se aplicara en los de recursos humanos y de los estudiantes. "Tenemos la presión de hacer más con la misma cantidad de personal, como muchas otras empresas. Pero cuando Ansible Automation Platform se encarga de las tareas repetitivas, las personas tienen más tiempo para trabajar en otros proyectos importantes", indicó Siegelman.

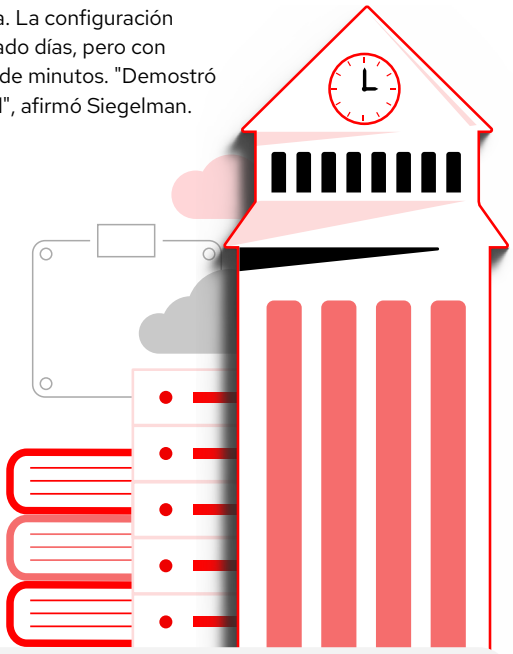
El personal de TI obtuvo más tiempo para adaptarse frente a los desafíos de la COVID-19

Otro ejemplo de la flexibilidad de Ansible Automation Platform sucedió en marzo de 2020 cuando Emory, como casi todas las universidades y empresas, debió cerrar sus instalaciones y enviar a los estudiantes y al personal a su hogar.

La OIT necesitaba implementar servidores de bases de datos rápidamente para gestionar el seguimiento de los empleados esenciales y otorgarles autorización para estar en el campus. El personal seleccionado completó cuestionarios que se ingresaron al sistema. La configuración manual de esta tarea en los servidores hubiera tomado días, pero con Ansible Automation Platform se realizó en cuestión de minutos. "Demostró lo que puede hacer la automatización en el backend", afirmó Siegelman.

Innovación de la seguridad más allá del campus con la automatización

La necesidad de automatizar es fundamental en los planes futuros de Emory, en especial en su transición a la nube. "Tenemos algunos sistemas heredados que son una combinación de estructuras viejas y nuevas, y estamos poniendo mucho esfuerzo en nuestra plataforma de AWS", mencionó Siegelman. "Con estos sistemas diferentes, Ansible Automation Platform nos permite tener procesos replicables que están estandarizados. No importa si la plataforma está en la nube o en las instalaciones, todo está en su lugar".



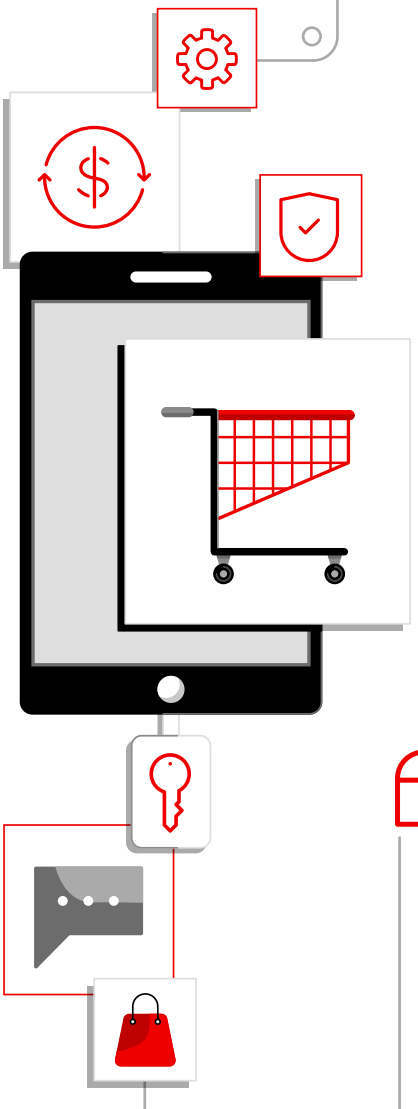
Descargue
el caso de éxito de Emory University

2

La empresa minorista Schwarz Group automatiza la TI con Red Hat Ansible Automation Platform

Schwarz Group es la cuarta empresa minorista más grande del mundo. Es oriunda de Alemania y opera en más de 12 500 tiendas en 33 países. Schwarz amplía rápidamente su presencia internacional y, para tener éxito, debe encontrar el equilibrio entre la gestión uniforme de las tiendas, la flexibilidad para adaptarse a las demandas locales y la agilidad para abrir otras tiendas rápidamente, particularmente en los mercados nuevos, al tiempo que reduce los riesgos.

Para administrar estas tiendas de manera uniforme y adaptarse con flexibilidad a la demanda local, el grupo migró de Puppet a Red Hat Ansible Automation Platform. Con una base operativa uniforme, puede usar funciones de autoservicio para implementar con rapidez los servicios digitales innovadores, mantener la competitividad y conservar una postura sólida de seguridad.



La uniformidad es la clave para la seguridad de miles de tiendas minoristas en todo el mundo

El equipo de TI de Schwarz cuenta con más de 3 500 ingenieros que respaldan más de 1 000 sistemas de SAP y 28 PB de almacenamiento alojado en centros de datos. Cada tienda de Schwarz opera Storeserver, un sistema operativo central instalado por el equipo de TI local de la empresa, el cual controla una variedad de funciones de las tiendas, desde los sistemas de caja y de circuito cerrado de televisión (CCTV) hasta los programas de reciclado y recompensas.

A fin de mejorar la gestión y la autorización de los usuarios y agilizar los procesos de implementación, el equipo de TI de Schwarz se propuso incorporar funciones de autoservicio controladas y eficientes. Para alcanzar este objetivo, implementó Ansible Automation Platform.

> *Debido a que los procesos son complejos y llevan mucho tiempo, la versión de la comunidad no cumplió con nuestras expectativas. La automatización es un elemento fundamental para nuestras operaciones, y el respaldo empresarial que brinda Red Hat fue uno de los motivos principales por los que nos decidimos por su solución.*
>
> Felix Kuehner, director del servidor para tiendas de los Servicios Esenciales de Infraestructura de la TI de Schwarz

Durante un taller de dos días, los equipos de TI de Schwarz trabajaron en conjunto con especialistas técnicos de Red Hat para revisar la arquitectura y establecer las prácticas recomendadas para la nueva solución de automatización.

Ahora, el grupo ejecuta más de 5 000 tareas de Ansible Automation Platform cada día para gestionar sus servidores en las tiendas.

Mejor gestión de los riesgos con el sistema de acceso basado en funciones

Gracias a Ansible Automation Platform, el equipo de TI de Schwarz mejoró su eficiencia para equilibrar el control del acceso al sistema de las aplicaciones autorizadas y el desarrollo con las funciones de autoservicio deseadas.
El control del acceso basado en funciones implica que los equipos de las aplicaciones pueden automatizar las implementaciones como usuarios comunes, sin la necesidad de acceder como superusuario a los sistemas centrales fundamentales para la empresa. "Esta función proporciona mayor uniformidad y permite que las personas trabajen de forma proactiva tanto en los proyectos nuevos como en los actuales", expresó Kuehner.

Luego del éxito inicial con Ansible Automation Platform, el equipo de TI de Schwarz planea seguir descubriendo formas nuevas de que las tiendas de la empresa operen de forma uniforme y, a la vez, tengan capacidad de respuesta.

> ***Valoramos el trabajo con Red Hat y esperamos que Ansible nos siga permitiendo encontrar otras maneras de modernizar nuestra empresa y mejorar su eficiencia.***
>
> Felix Kuehner, director del servidor para tiendas de los Servicios Esenciales de Infraestructura de la TI de Schwarz

Descargue
el caso de éxito de Schwarz

Agile Defense mejora el cumplimiento normativo de la seguridad con Red Hat Ansible Automation Platform

3

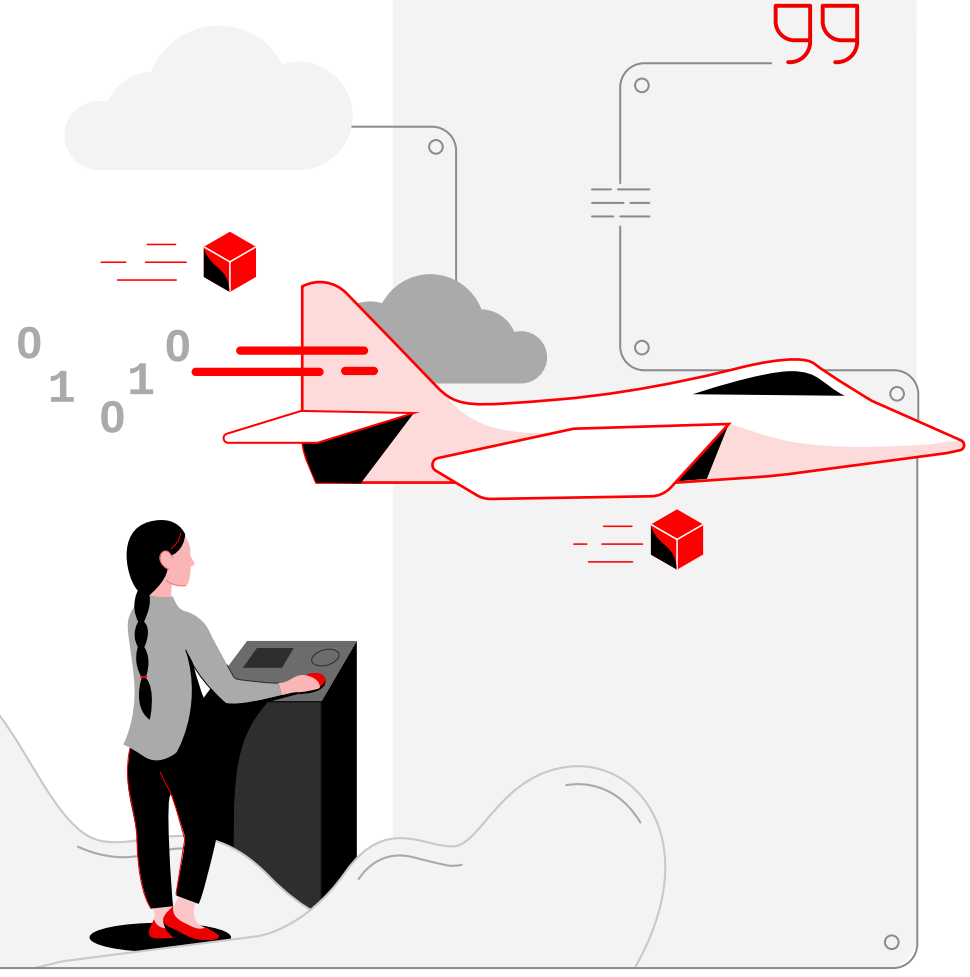
Agile Defense es una empresa líder en servicios de tecnología de la información ubicada en Reston, Virginia. Cuenta con muchos clientes del gobierno de los EE. UU., entre los que se incluyen varias agencias civiles y sucursales dentro del Departamento de Defensa de los EE. UU. Por lo tanto, la seguridad de la TI es la principal prioridad.

Nunca fue más pertinente evitar que los criminales cibernéticos obtengan acceso no autorizado a los sistemas y la infraestructura. Muchas de las filtraciones que suceden son el resultado de errores de configuración. Para el Departamento de Defensa (DoD) de los EE. UU. y las agencias federales, la tarea de evitar las amenazas requiere que cumplan con estándares estrictos relacionados con la información, la seguridad, la configuración y el cumplimiento normativo en la Agencia de Sistemas de Información de Defensa (DISA).

Las auditorías regulares para detectar errores de configuración y de otra índole son parte de la tarea, pero son repetitivas, costosas y demandan muchos recursos. Las agencias pueden pasar meses preparándose para una auditoría.

El enfoque manual y reactivo sobre esta tarea dejaba a sus clientes expuestos a puntos vulnerables conocidos en el periodo entre las verificaciones.

> ***Las tareas de producción de nuestros clientes solían interrumpirse mientras se reunía toda la documentación antes de una inspección.***
>
> Shawn Draper, ingeniero de soluciones en Agile Defense



El uso de la automatización para reducir el impacto de las auditorías

Los errores de configuración y las auditorías son dificultades generales para muchos de los clientes gubernamentales de Agile Defense. La empresa líder en servicios de TI, que se enorgullece de innovar gracias a la tecnología de la información, se asoció con Red Hat para crear una herramienta de configuración, notificación y solución con la Guía técnica de implementación de seguridad (STIG). Esta solución de automatización realiza auditorías específicas de los sistemas, cuenta con la opción de corregir errores de configuración e informa el estado actual de los dispositivos. También conocida como cumplimiento como servicio (CPaaS) de Agile Defense, la solución STIG utiliza Red Hat Ansible Automation Platform debido a sus funciones de automatización flexibles y con capacidad de ajuste.

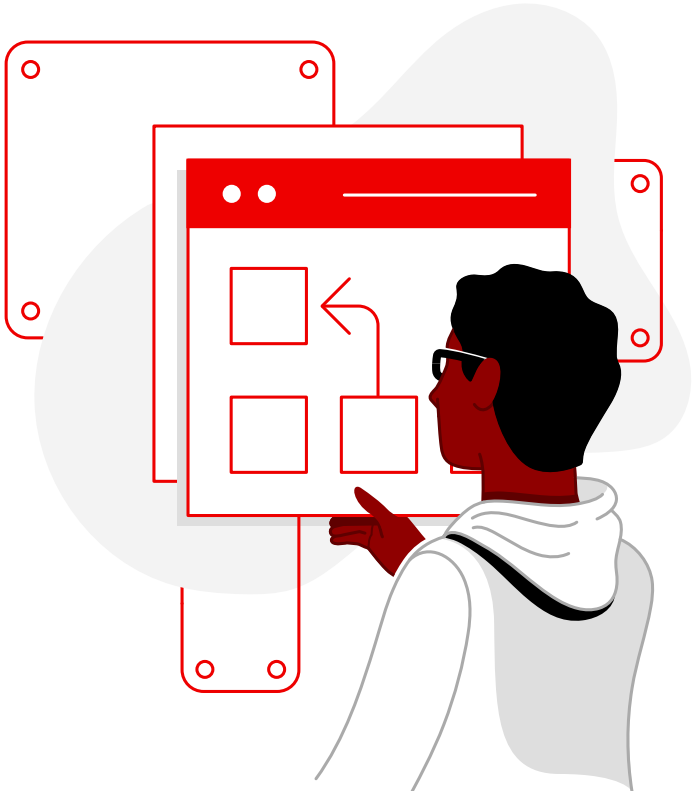
Asimismo, Red Hat colaboró con DISA en una STIG para Red Hat Enterprise Linux y conoce la importancia de crear estándares para cada versión de software, dispositivo y sistema operativo.

> ***Elegimos Red Hat Ansible Automation Platform para resolver este problema porque puede comunicarse con todo.***
>
> Shawn Draper, ingeniero de soluciones en Agile Defense

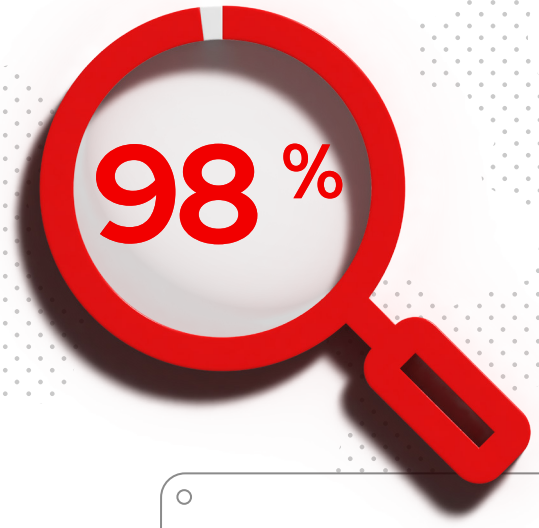
Las ventajas de seguridad de los playbooks de Ansible

El CPaaS utiliza las funciones de automatización de la gestión de la configuración de Red Hat Ansible Automation Platform para auditar los puntos vulnerables abiertos. "Red Hat Ansible Automation Platform se conecta a los dispositivos y ejecuta comandos especificados en un playbook de Ansible", indicó Draper.

Luego de identificar los errores de configuración de manera automática, el CPaaS también puede corregirlos siguiendo los comandos en un playbook de Ansible personalizado. Agile Defense diseñó una variedad de playbooks para evaluar diferentes tipos de dispositivos, entre los que se incluyen las plataformas de Red Hat, los dispositivos de Windows, los hipervisores de VMware, los enrutadores y conmutadores de Cisco y los firewalls.



El tiempo que necesitaban los clientes para realizar las auditorías se redujo un



El CPaaS produce toda la documentación necesaria de manera automática. Específicamente, el CPaaS utiliza Ansible Automation Platform para escribir un archivo de control XML (que se puede ver en el visualizador de la STIG de DISA) para cada dispositivo en la red y cada punto vulnerable identificado para presentar al auditor. Estos artefactos pueden mostrar la información del estado actual y demostrar que se implementaron ciertas configuraciones de seguridad. Ansible Automation Platform también permite que los clientes extiendan las funciones de CPaaS para gestionar flujos de trabajo e inventarios, programar auditorías e incorporar el control del acceso basado en funciones. El CPaaS también garantiza la uniformidad en todos los dispositivos.

> ***Uno de los mejores aspectos de la automatización es que hace lo mismo cada vez.***
>
> Shawn Draper

La supervisión anticipada de la postura de seguridad de las agencias que proporciona el CPaaS es fundamental para mantenerse preparado para las amenazas cibernéticas. Históricamente, esta tarea requería muchos recursos y sistemas de software adicionales en los dispositivos del extremo. Con el uso de Ansible Automation Platform para analizar los puntos vulnerables abiertos, el CPaaS de Agile Defense les ahorra a los clientes del gobierno un 98 % del tiempo que pasan en las auditorías.

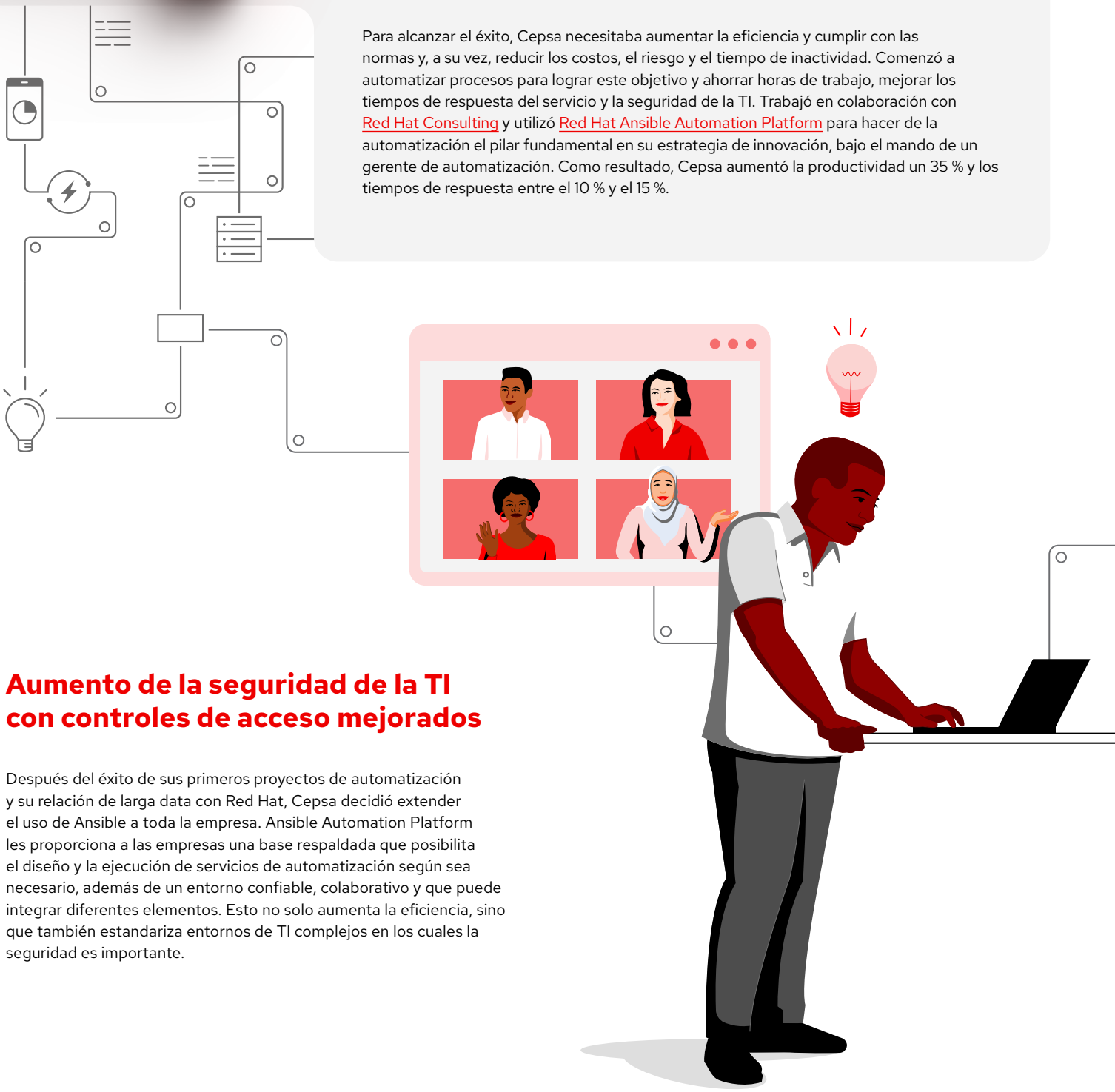
Descargue
el caso de éxito de Agile Defense

4

Cepsa mejora la eficiencia con Red Hat Ansible Automation Platform

La empresa global de energía y productos químicos Cepsa se encuentra en una misión hacia la reducción de la huella de carbono en todo el mundo. En 2022, presentó su estrategia para ser líder en movilidad sostenible, biocombustibles e hidrógeno ecológico, con el foco en España y Portugal, y una referencia clave en la transición energética.

Para alcanzar el éxito, Cepsa necesitaba aumentar la eficiencia y cumplir con las normas y, a su vez, reducir los costos, el riesgo y el tiempo de inactividad. Comenzó a automatizar procesos para lograr este objetivo y ahorrar horas de trabajo, mejorar los tiempos de respuesta del servicio y la seguridad de la TI. Trabajó en colaboración con Red Hat Consulting y utilizó Red Hat Ansible Automation Platform para hacer de la automatización el pilar fundamental en su estrategia de innovación, bajo el mando de un gerente de automatización. Como resultado, Cepsa aumentó la productividad un 35 % y los tiempos de respuesta entre el 10 % y el 15 %.



Aumento de la seguridad de la TI con controles de acceso mejorados

Después del éxito de sus primeros proyectos de automatización y su relación de larga data con Red Hat, Cepsa decidió extender el uso de Ansible a toda la empresa. Ansible Automation Platform les proporciona a las empresas una base respaldada que posibilita el diseño y la ejecución de servicios de automatización según sea necesario, además de un entorno confiable, colaborativo y que puede integrar diferentes elementos. Esto no solo aumenta la eficiencia, sino que también estandariza entornos de TI complejos en los cuales la seguridad es importante.

La sintaxis fácil de comprender del playbook de Ansible permitió que Cepsa definiera los parámetros de seguridad para todas las partes del sistema, ya sea que se relacionaran con el establecimiento de reglas de firewall, el bloqueo de usuarios y grupos o la aplicación de políticas personalizadas de seguridad. La estandarización de los procesos ayudó a Cepsa a reducir la cantidad de permisos administrativos adicionales para la seguridad en sus sistemas, lo cual disminuyó el riesgo. En la actualidad, agrupa a los usuarios según el puesto de trabajo y el departamento para asegurarse de otorgar solo los niveles de permiso indicados, sin conceder accesos adicionales.

Como resultado, Cepsa aumentó la productividad un 35 % y los tiempos de respuesta entre el 10 % y el 15 %.

Ahora, los técnicos pueden acceder a Ansible Automation Platform y reiniciar el servicio sin las credenciales, lo cual les garantiza que el proceso se ejecutará de la manera descrita en el código predefinido.

La productividad
aumentó un **35 %**

Los tiempos de respuesta
aumentaron entre **10 y 15 %**

La automatización contribuyó a un cambio cultural positivo que mejoró la colaboración entre los equipos. Red Hat colabora con nosotros para implementar las prácticas recomendadas y para que aprendamos de su experiencia en toda la empresa.

Francisco José Martín, gerente de automatización del Departamento de Explotaciones y Operaciones de Cepsa.

Un cambio hacia una cultura centrada en la seguridad con la orientación de los especialistas en automatización

Red Hat Consulting ayudó a Cepsa a implementar los cambios que necesitaba para aprovechar al máximo la tecnología de automatización y el enfoque que acababan de adoptar. Los especialistas de Red Hat trabajaron junto con el equipo de la empresa y pudieron demostrar los beneficios de un enfoque de trabajo ágil y la mejora permanente de la calidad mediante la integración y la distribución continuas (CI/CD).

Descargue
el caso de éxito de Cepsa

5

SIEMENS

Siemens mejora la seguridad de la comunicación con Red Hat Ansible Automation Platform

Siemens se ubica en Munich, Alemania, y es la empresa de ingeniería más grande de Europa. El grupo mundial de tecnología se dedica a la electrificación, desde la generación, la transmisión y la distribución de energía hasta las soluciones de redes inteligentes y la aplicación eficiente de energía eléctrica.

Debido a la naturaleza sensible de sus operaciones comerciales, Siemens se compromete a mantenerse a la vanguardia de la tecnología de la seguridad. Para proteger con confianza el acceso a la información confidencial, sus 295 000 empleados y los 100 000 empleados de sus partners empresariales utilizan infraestructuras de clave pública (PKI), y controlan los certificados y la identidad de las claves públicas. El incremento del uso de esta tecnología tiene como fin proteger también la comunicación del Internet de las cosas (IoT), así que ahora mantiene dos entornos de PKI para sus diferentes casos prácticos de aplicaciones.

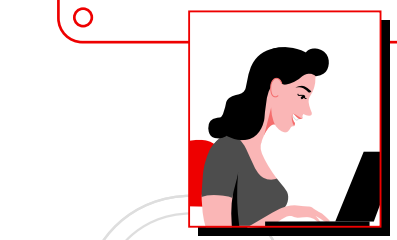
> *Esto es particularmente importante, ya que la infraestructura como código con Red Hat Ansible Automation Platform es más que la incorporación de una herramienta nueva, sino que requiere un cambio fundamental en el enfoque de los administradores de sistemas.*
>
> Rufus Buschart, director de infraestructura de clave pública (PKI), Siemens

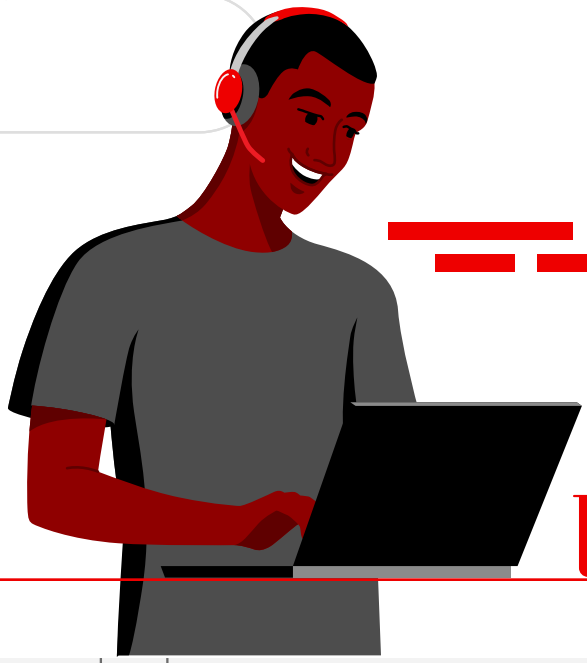
Siempre que necesitamos a Red Hat, están ahí, y nuestra visión es trabajar juntos para desarrollar una plataforma de prácticas recomendadas de automatización para optimizar la eficiencia y la innovación de nuestra empresa.

Rufus Buschart

A medida que las comunicaciones entre los equipos de servicios de la empresa se expanden, la complejidad de la configuración también aumenta para el equipo de PKI de Siemens. Para respaldar esta demanda, la empresa reemplazó su solución de automatización heredada con Ansible Automation Platform.

Gracias a Ansible Automation Platform, Siemens ahora puede automatizar tareas administrativas, aumentar la calidad de la configuración y mejorar la seguridad de la comunicación en toda la empresa. Además, disfrutó de las ventajas de la experiencia de Red Hat y planifica trabajar con la empresa para explorar la automatización de los procesos de pruebas, con el objetivo de establecer un entorno común para la implementación constante.





Descargue
el caso de éxito de Siemens

Con-clusión

Ansible Automation Platform ayuda a las empresas a gestionar los sistemas de seguridad automatizados para anticiparse a los ataques maliciosos. Ansible cuenta con acceso a miles de módulos para ayudar a los equipos a automatizar todos los aspectos de su entorno y sus procesos de TI, y puede integrar muchos equipos para proteger los perímetros complejos de seguridad, lo que permite unificar el enfoque y mejorar la postura de seguridad.

Con Ansible Automation, los equipos de seguridad pueden:

Unir los flujos de trabajo y los playbooks para poder reutilizarlos en forma modular.

Los equipos de seguridad pueden configurar una secuencia de tareas que compartan el inventario, los playbooks o los permisos para automatizar por completo las investigaciones o las correcciones.

Consolidar y centralizar los registros.

La integración con los servicios de terceros que agrupan registros externos a la plataforma permite que los equipos de seguridad identifiquen las tendencias, analicen los eventos de la infraestructura, supervisen las anomalías y establezcan relaciones entre los diferentes eventos.

Admitir los controles de acceso y los servicios del directorio local.

La suma de los servicios de directorio de los usuarios y la infraestructura permite que los equipos de seguridad centralicen el acceso a las tareas y su ejecución, asignen subconjuntos de operaciones a funciones específicas y compartan tareas con otros grupos.

Integrar aplicaciones externas con API de RESTful

Los equipos de seguridad pueden utilizar esta plataforma para gestionar otras aplicaciones empresariales, como las soluciones de organización, automatización y respuesta de la seguridad (SOAR).

Mejore su postura de seguridad con la automatización.

Obtenga más información
sobre Red Hat Ansible Automation Platform.

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800