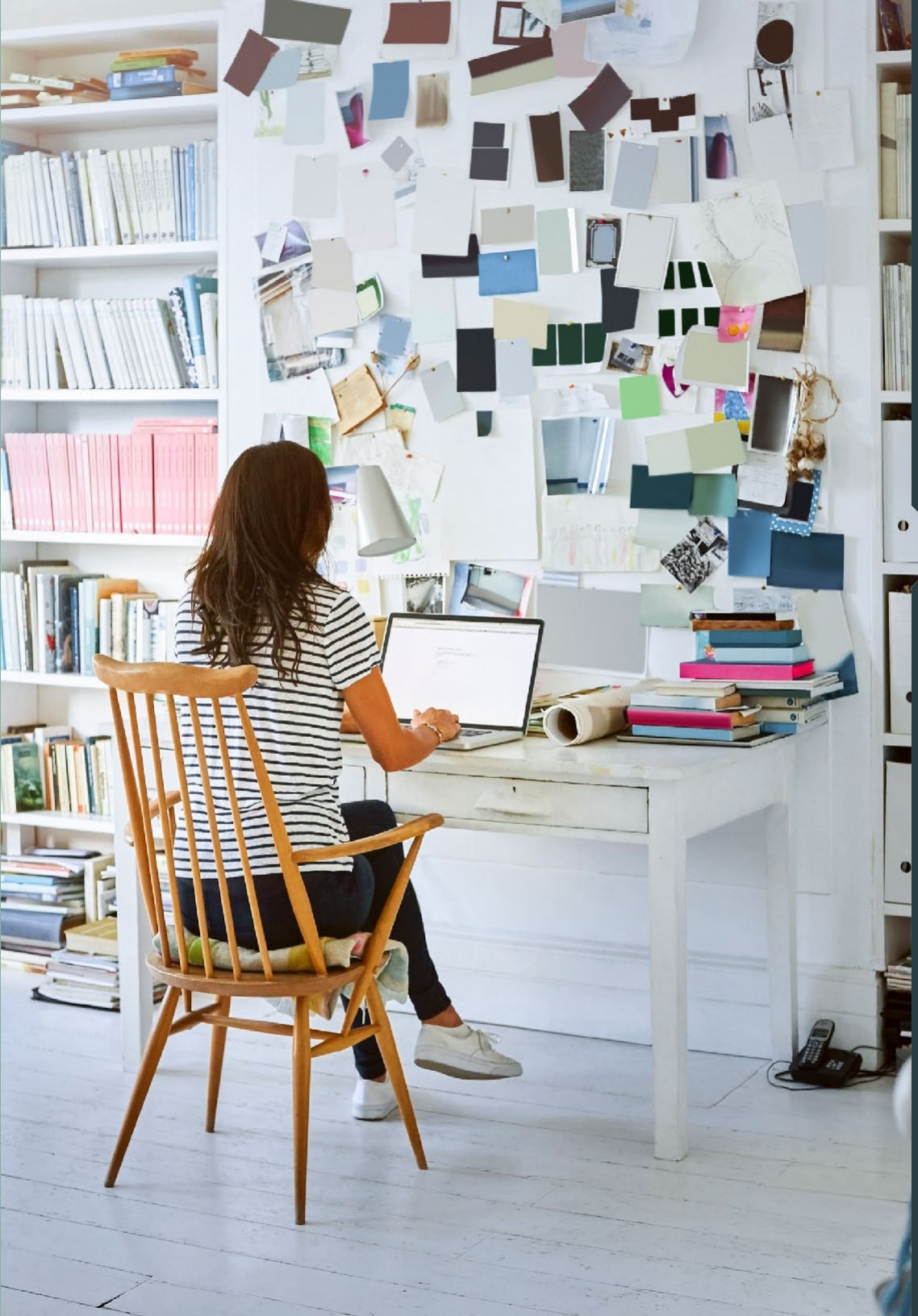


servicenow

Ahora todos juntos

Mejora de la colaboración entre los equipos de TI y seguridad para impulsar la resiliencia operativa.

EMPEZAR »

La tormenta perfecta

En 2020, la seguridad se complicó mucho. Los ciberdelincuentes aumentaron su actividad, ansiosos por aprovechar la situación de confusión y sacar partido de la pandemia.

El volumen de correos electrónicos de phishing, disfrazados de mensajes urgentes sobre la COVID-19, aumentó casi un 6,654 % en solo dos meses. Desde enero, se registraron más de 100 000 dominios relacionados con el coronavirus en todo el mundo, con un 50 % más de probabilidades de que estos dominios hospedasen malware.

Esto se sumó a las amenazas tradicionales, como el ransomware, que se prevé que este año supongan más de 1300 millones de dólares para los ciberdelincuentes, o las estafas a través del correo electrónico empresarial que sumaron pérdidas para las víctimas de más de 1700 millones de dólares en 2019.

Al aumento del número y la velocidad de las amenazas se suma el hecho de que la mayoría de las organizaciones ha respondido a la crisis permitiendo a sus empleados trabajar desde sus casas, lo que ha dado lugar a una "tormenta perfecta". Con una fuerza laboral distribuida, el perímetro de la red tradicional se desvanece. Desde una perspectiva operativa, era un cambio esencial, pero para la seguridad supuso una extraordinaria ampliación de la superficie de ataque que se debía proteger.

La necesidad de actuar con rapidez y responder a los riesgos y las amenazas nunca ha sido mayor. Y el tiempo es un bien de lujo que los equipos de seguridad no tienen: se tarda de media 73 días en contener una brecha de seguridad, con un coste total medio de 3,92 millones de dólares.

No se puede arreglar lo que no se ve

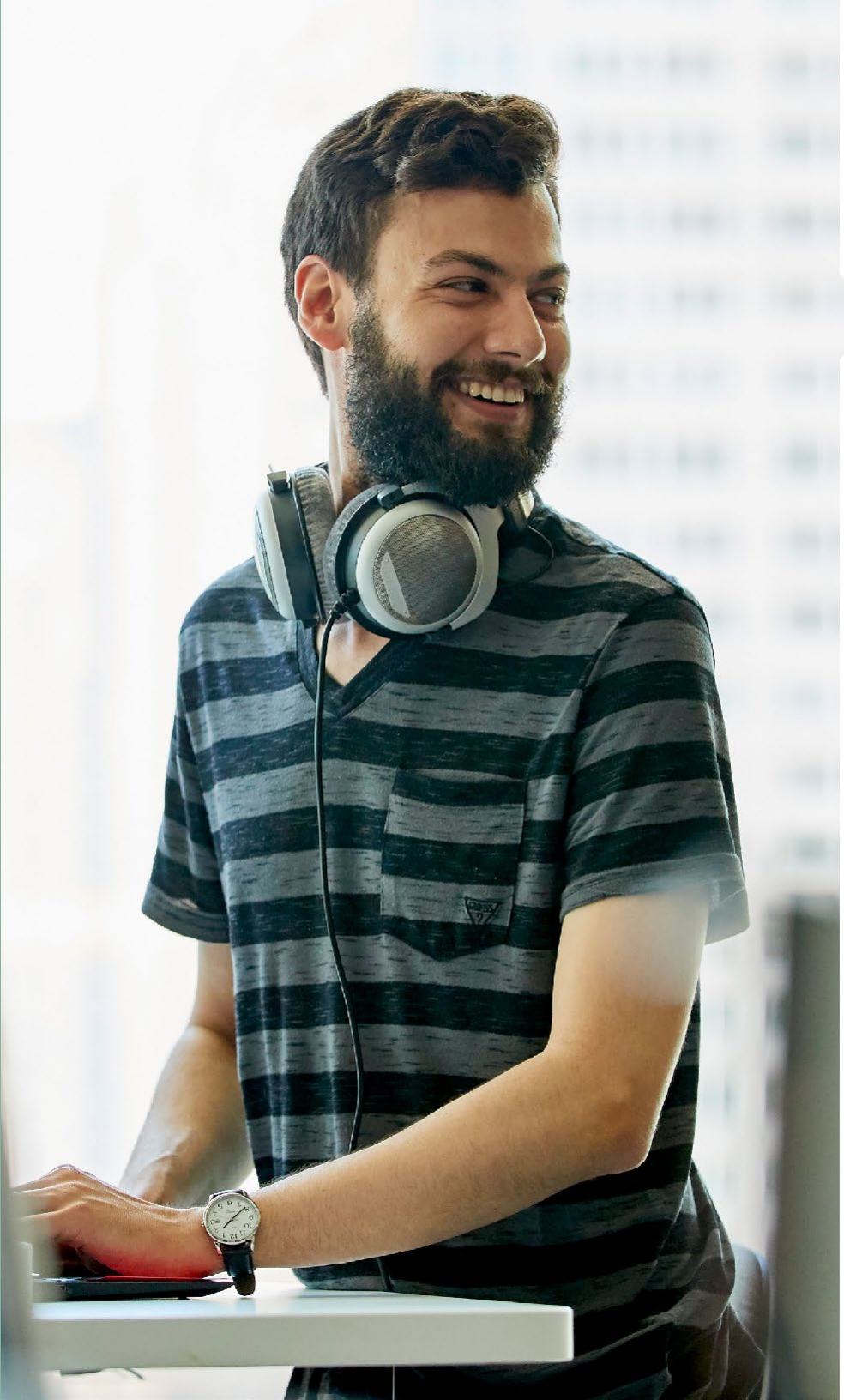
Proteger los activos más valiosos de una organización y reducir el riesgo de pérdida financiera y daños en la reputación es más importante que nunca. Pero para priorizar las acciones y responder de manera eficaz, los equipos de TI y seguridad deben tener visibilidad de los incidentes y del contexto empresarial.

Estos son algunos de los obstáculos que encuentran muchas organizaciones:

- Datos aislados
- Falta de recursos
- No aplicar parches en vulnerabilidades conocidas
- Dependencia de procesos manuales
- Mínima cooperación entre los equipos de seguridad y TI

Estas trabas reducen la velocidad de respuesta ante las nuevas amenazas que surgen constantemente, lo que agrava aún más el problema:

- Conocimiento insuficiente del panorama de amenazas
- Incapacidad para priorizar las amenazas de forma rápida y precisa
- Respuesta demasiado lenta y demasiado aislada para evitar el impacto en el negocio



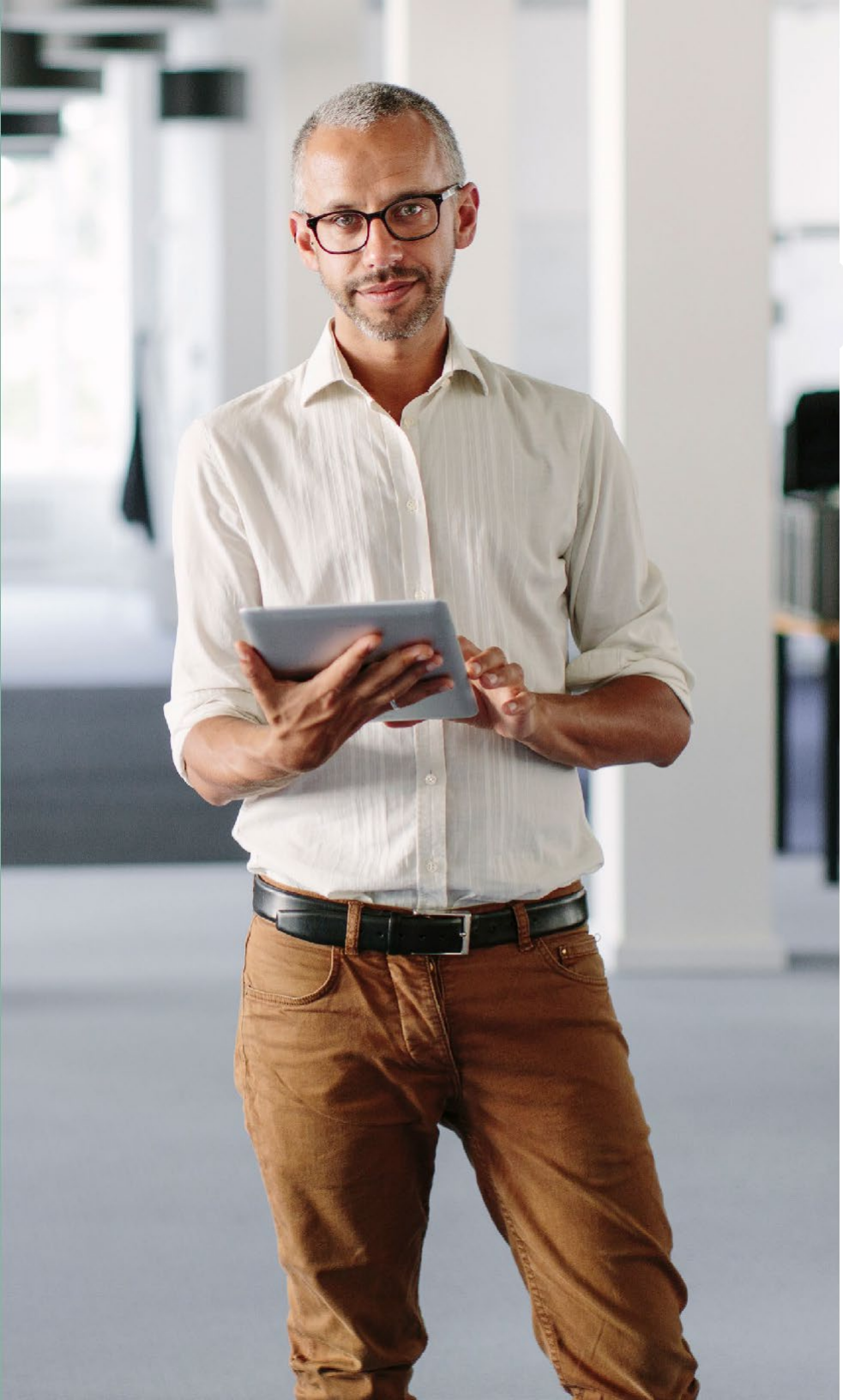
Eliminar los obstáculos que frenan la resiliencia

Para construir una organización más resiliente, se requiere confianza en cada etapa del viaje. Esto exige una colaboración más estrecha entre los equipos de seguridad y TI con el fin de maximizar la productividad y minimizar los riesgos.

Es ahí donde entra en juego un enfoque de circuito cerrado. Es una manera de crear una organización realmente resiliente que pueda protegerse a sí misma, independientemente de lo que esté sucediendo en un entorno más amplio. Es un enfoque de cuatro pasos que ofrece las siguientes ventajas:

- Obtener visibilidad de los incidentes para controlarlos mejor
- Planificar y priorizar las tareas esenciales según su importancia
- Optimizar y colaborar en relación con los riesgos y amenazas para la organización
- Impulsar la productividad entre equipos en toda la empresa

Abordaremos cada uno de estos cuatro aspectos principales en las siguientes páginas. Pero antes de eso, veamos cuál es el concepto que todos ellos comparten.

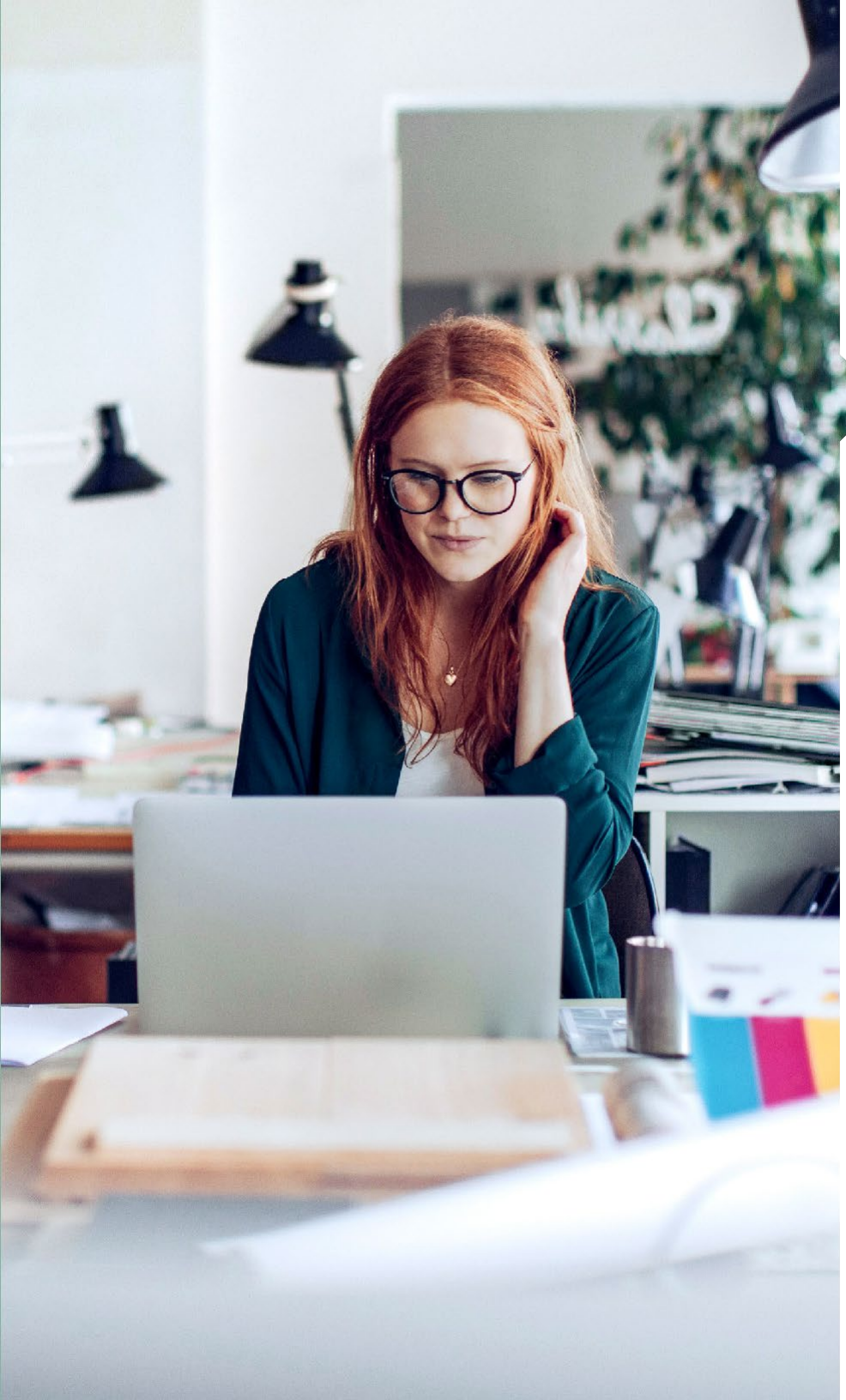


Aceleración del tiempo de respuesta

Las organizaciones se preocupan con razón por el coste financiero de una filtración de datos. Cuando se depende de procesos manuales y flujos de trabajo aislados, es mucho más difícil reaccionar con rapidez y saber qué solución ha sido eficaz para poder repetirla la próxima vez.

Es ahí donde pueden ayudar las soluciones de seguridad automatizadas que utilizan la inteligencia artificial, el aprendizaje automático, los análisis de seguridad y la respuesta orquestada a incidentes. Minimizan la necesidad de intervención humana y se ha demostrado que reducen los costes asociados a un incidente de seguridad o a una filtración de datos.

Automatizar los flujos de trabajo, además de compartir datos y acciones entre los equipos de seguridad y TI, ayuda a garantizar que las amenazas a la empresa se resuelvan antes de que afecten seriamente a su actividad.



El tiempo es oro

La automatización y la colaboración dan lugar a respuestas eficientes e impulsan la resiliencia operativa: el 80 % de las organizaciones que utilizan la automatización son capaces de responder a las vulnerabilidades en menos tiempo.

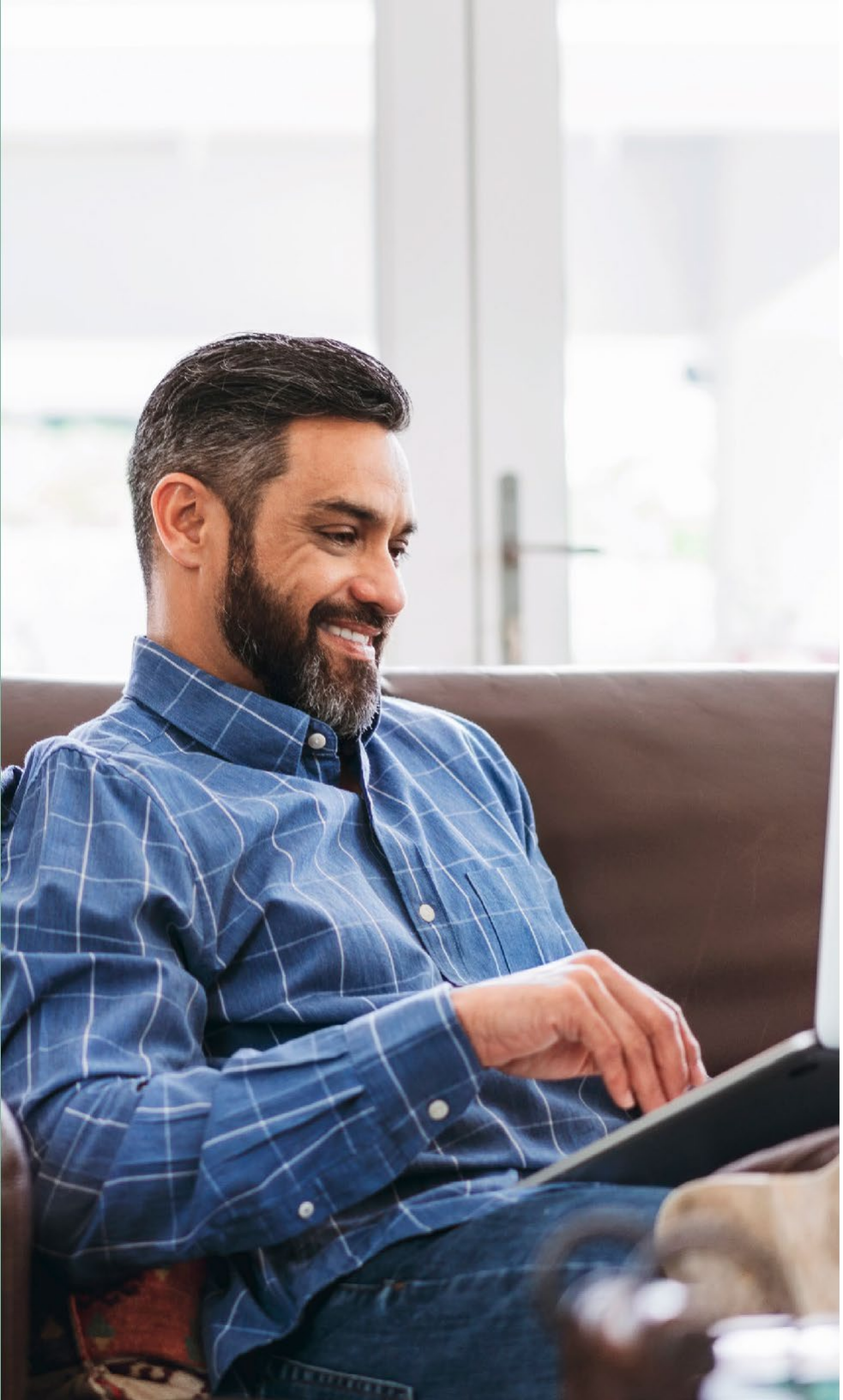
Para las organizaciones que no han automatizado la seguridad, los costes de las infracciones fueron considerablemente más elevados que para aquellas que habían desplegado completamente la automatización (coste medio total de 5,16 millones USD de una infracción sin automatización frente a 2,65 millones USD con una automatización plenamente desplegada).

Y las tendencias siguen una sola dirección: el coste medio de una infracción para las organizaciones sin automatización fue mayor en 2019 que en 2018 (un aumento de más del 16 %, de 4,43 millones a 5,16 millones USD).

El coste de los ataques a organizaciones con una automatización total se redujo de 2018 a 2019. El coche de las brechas cayó en un 8 %, de una media de 2,88 millones USD en 2018 a 2,65 millones USD en 2019.

Reto	Solución	Herramientas
Datos aislados El 76 % de las organizaciones no ofrece una vista común de los activos y aplicaciones a sus equipos de seguridad y TI. Algunas de las mayores amenazas a la seguridad aprovechan vulnerabilidades conocidas. Sin embargo, cuando el SOC medio contiene 75 herramientas diferentes y cada una de ellas genera alertas, es difícil distinguir las señales reales del ruido y aún más difícil escalar los problemas a las personas correctas para actuar rápidamente y reducir el riesgo de inactividad.	**Planificar y priorizar las tareas esenciales según su importancia** Con visibilidad completa, los equipos de seguridad pueden conocer su estado de seguridad y obtienen el contexto empresarial que necesitan para distinguir las amenazas de alto impacto del ruido que está ocurriendo en ese momento y conseguir que las operaciones sigan funcionando sin problemas.	**Respuesta a incidentes de seguridad** Simplifica la identificación de incidentes críticos y proporciona herramientas de flujo de trabajo y automatización para acelerar la remediación. Conecta las competencias de automatización y de flujo de trabajo de Now Platform™ con datos de seguridad de los principales proveedores para darle a tus equipos una plataforma única de respuesta compartida entre los departamentos de seguridad y TI. **Respuesta a la vulnerabilidad** Permite priorizar eficientemente los esfuerzos de aplicación de parches relacionándolos con el impacto empresarial. Con orquestación, automatización y mejor visibilidad, los equipos pueden responder de manera más eficiente, reduciendo el riesgo empresarial.
Falta de recursos El 82 % de los empleadores afirma no tener suficientes expertos en ciberseguridad. Los procesos manuales están dificultando la capacidad de supervisar de forma continua los cambios en las amenazas y vulnerabilidades, así como las nuevas, a medida que surgen. En un momento de alta demanda de expertos en seguridad, muchas organizaciones no pueden permitirse el lujo de asignar más personal para resolver los problemas.	**Supervisión continua** Gracias a la automatización, es posible identificar los cambios de seguridad en tiempo real y responder con la velocidad de una máquina con el fin de priorizar las amenazas y vulnerabilidades más apremiantes, aprovechando así al máximo los recursos disponibles.	**Respuesta a incidentes de seguridad** Simplifica la identificación de incidentes críticos y proporciona herramientas de flujo de trabajo y automatización para acelerar la remediación. Conecta las competencias de automatización y de flujo de trabajo de Now Platform™ con datos de seguridad de los principales proveedores para darle a tus equipos una plataforma única de respuesta compartida entre los departamentos de seguridad y TI. Con orquestación, automatización y mejor visibilidad, los equipos pueden responder de manera más eficiente, reduciendo el riesgo empresarial. **Integrated Risk Management** Habilita un análisis de impacto empresarial detallado, además de priorizar de forma apropiada los riesgos y responder a ellos. **Gestión de vulnerabilidades** Los sistemas analizan los activos para identificar vulnerabilidades o debilidades que pueden ser aprovechadas por los atacantes y potencialmente dar lugar a una violación de seguridad.

Reto	Solución	Herramientas
Colaboración entre departamentos El 62 % de las organizaciones que han sufrido una filtración de datos ni siquiera sabía que era vulnerable. Ahora que muchos equipos se encuentran dispersos geográficamente debido a las nuevas normas de trabajo, la posibilidad de colaborar más estrechamente se reduce. La naturaleza aislada de los departamentos obstaculiza los esfuerzos de los equipos de seguridad y TI por colaborar y compartir información.	**Optimizar y colaborar en relación con los riesgos y las amenazas** Es importante crear flujos de trabajo abiertos en los equipos de seguridad y TI para agilizar la respuesta reduciendo los procesos engorrosos y los traspasos manuales durante los procesos de respuesta y corrección.	**Respuesta a incidentes de seguridad** Simplifica la identificación de incidentes críticos y proporciona herramientas de flujo de trabajo y automatización para acelerar la remediación. Conecta las competencias de automatización y de flujo de trabajo de Now Platform™ con datos de seguridad de los principales proveedores para darle a tus equipos una plataforma única de respuesta compartida entre los departamentos de seguridad y TI. **Respuesta a la vulnerabilidad** Permite priorizar eficientemente los esfuerzos de aplicación de parches relacionándolos con el impacto empresarial. Con orquestación, automatización y mejor visibilidad, los equipos pueden responder de manera más eficiente, reduciendo el riesgo empresarial y ampliando la capacidad del equipo.
Excesiva dependencia de procesos manuales El 56 % de las organizaciones afirma que los eventos pasan inadvertidos porque se utilizan correos electrónicos y hojas de cálculo para la respuesta a incidentes. Existe una incapacidad de identificar la causa raíz de los eventos pasados con el fin de mejorar los controles y las políticas, y fortalecer las operaciones. Esto da lugar a la repetición de los mismos riesgos y amenazas, así como a tareas manuales repetitivas por parte de los equipos de seguridad.	**Medidas de respuesta más inteligentes y repetibles** Se deben automatizar los flujos de trabajo multifuncionales y la recopilación de pruebas, y poner fin a los procesos que consumen mucho tiempo y son propensos a errores: el correo electrónico, las hojas de cálculo o las llamadas telefónicas.	**Respuesta a incidentes de seguridad** Simplifica la identificación de incidentes críticos y la respuesta a ellos, y proporciona herramientas de flujo de trabajo y automatización para acelerar la remediación. Conecta las competencias de automatización y de flujo de trabajo de Now Platform™ con datos de seguridad de los principales proveedores para darle a tus equipos una plataforma única de respuesta compartida entre los departamentos de seguridad y TI. **Respuesta a la vulnerabilidad** Permite priorizar eficientemente los esfuerzos de aplicación de parches relacionándolos con el impacto empresarial. Con orquestación, automatización y mejor visibilidad, los equipos pueden responder de manera más eficiente, reduciendo el riesgo empresarial y ampliando los recursos del equipo.

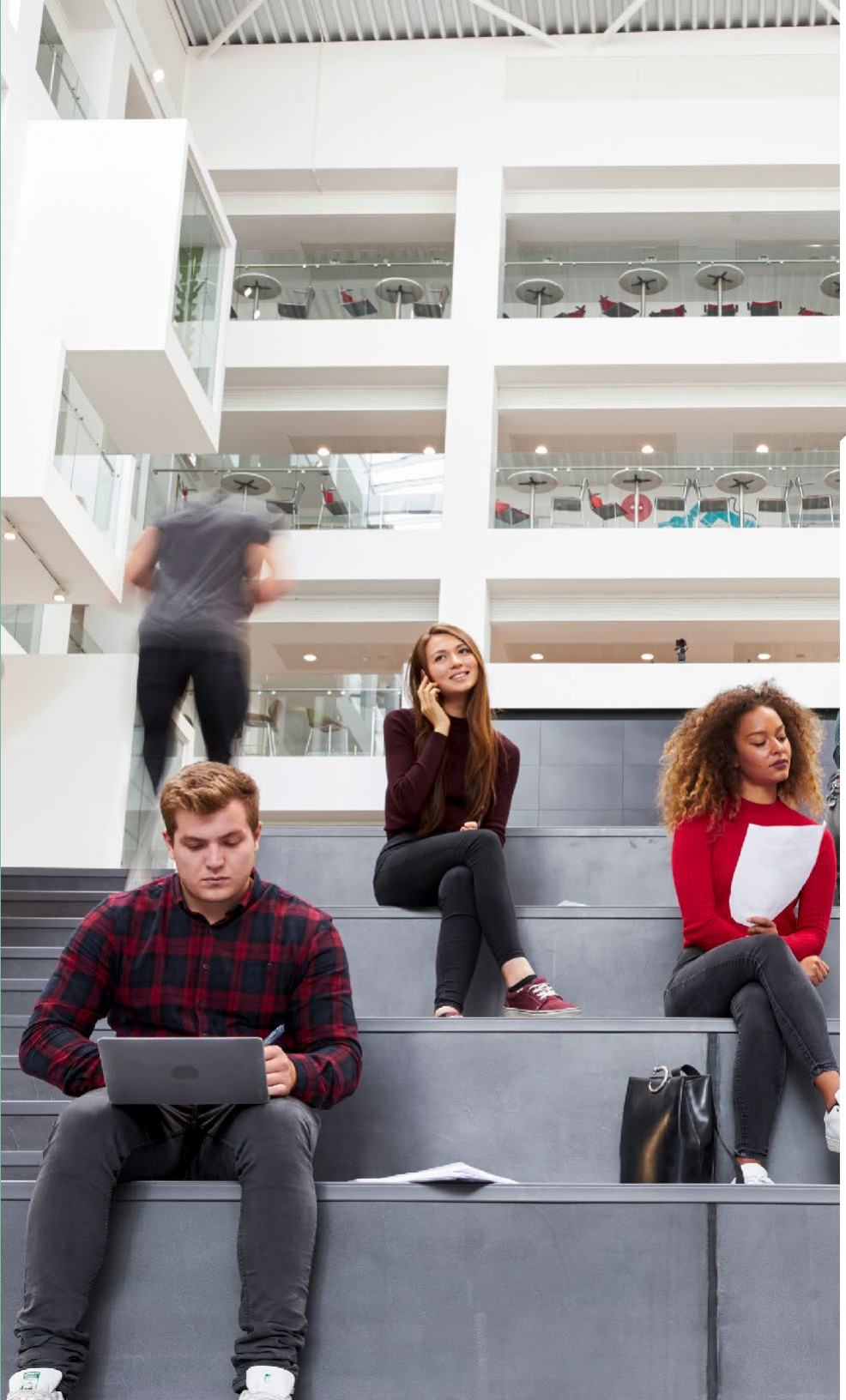


Juntos podemos encontrar la solución

Cuando los equipos de seguridad y TI trabajan en armonía, pueden impulsar mejoras continuas, de modo que la empresa pueda ir siempre un paso por delante de las amenazas más recientes.

Utiliza procesos precisos y repetibles para personalizar los Playbooks y las políticas con el fin de ofrecer respuestas automatizadas y más inteligentes que generen nuevas eficiencias. Esto crea una cultura que nunca deja de aprender, adaptarse y generar informes, lo que finalmente conduce a operaciones de seguridad más sólidas y preparadas para el futuro.

Puedes tener la certeza de que al vincular la acción humana con la inteligencia artificial y la automatización, estarán cubiertos todos los ángulos, sin importar cuáles sean las amenazas o dónde se encuentren los equipos.



Automatización en acción: historias de éxito reales

Tiempos de respuesta reducidos

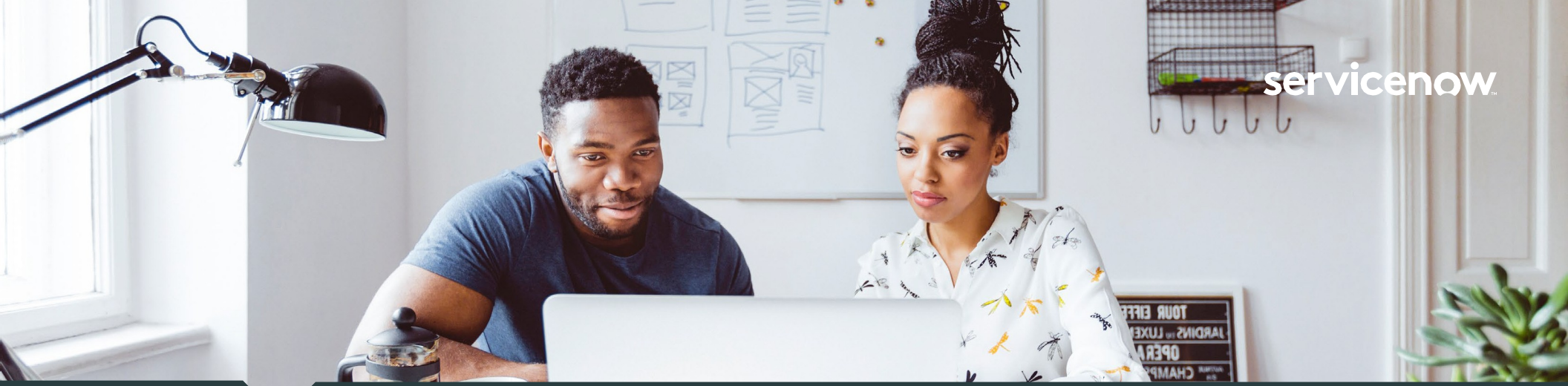
AMP, una empresa australiana de servicios financieros, se asoció con ServiceNow para implementar una solución de operaciones de seguridad que les permitió reducir en un 60 % el tiempo de respuesta y corrección de vulnerabilidades.

Investigación de seguridad más rápida

Gracias a Threat Intelligence, la empresa internacional de servicios de TI DXC redujo a la mitad el tiempo necesario para investigar los incidentes de seguridad.

Mayor eficiencia

Aplicando la automatización de sus propios productos, ServiceNow ayudó a su equipo de seguridad a gestionar un 50 % más de casos.



Mejorar constantemente

ServiceNow proporciona conocimientos acerca del contexto empresarial y la gravedad de los problemas en una sola plataforma donde poder evaluar la situación de forma precisa y rápida. Esto permite lo siguiente:

- **Centrar** los esfuerzos en los incidentes con el mayor impacto potencial.
- **Priorizar** los incidentes y vulnerabilidades de seguridad en función de la importancia para el negocio.
- **Mejorar** la toma de decisiones para que los esfuerzos de respuesta sean más rápidos y eficaces.
- **Alinear** los datos correctos con las personas adecuadas.
- **Rastrear** los incidentes y asignar tareas a los responsables pertinentes.
- **Garantizar** que las tareas se completan a tiempo.

Security Operations es una plataforma única integrada que permite a los diferentes equipos correlacionar rápidamente eventos de seguridad, identificar dependencias entre sistemas y automatizar la interacción entre las tareas y el flujo de trabajo del sistema en toda la empresa con el fin de priorizar y alinear las respuestas a las amenazas y vulnerabilidades antes de que la empresa se vea afectada.

Gracias a la combinación de las capacidades de Security Operations y las soluciones de TI, los equipos pueden responder de manera más rápida y eficaz, lo que reduce los riesgos empresariales.

El fin de la tecnología no es reemplazar a los humanos en materia de seguridad, sino ayudarles a optimizar su trabajo.

Ver ahora

« ATRÁS