El componente humano de la ciberseguridad

Piense en el peor de los casos.

Un sofisticado ataque de ransomware apaga su centro de datos. Los servicios de ventas, atención al cliente y finanzas quedan inoperativos. Es su responsabilidad restaurar los sistemas, pero, aunque tiene grandes conocimientos y experiencia en TI, no consigue encontrar una solución.

Su reducido equipo lleva varias semanas trabajando con muy poco descanso o tiempo libre. Algunos miembros han ***estado en su puesto hasta 36 horas seguidas*** sin dormir. Le preocupa que el cansancio esté haciendo que la toma de decisiones sea deficiente, algo que podría poner en riesgo el esfuerzo de recuperación.

Necesita desesperadamente más recursos que puedan intervenir inmediatamente y abordar el problema, pero no sabe dónde encontrarlos.

Esta situación puede parecer el comienzo de una novela, pero se basa en las experiencias reales de los clientes de Dell. Pone de relieve un problema importante en el entorno de ciberseguridad actual: el factor humano.

Datos recientes indican que el sector sufre una escasez de casi 5 millones de profesionales de la seguridad. Aunque la necesidad de recursos es más notable durante un incidente, las soluciones se encuentran atendiendo a las causas reales.

Empiece por crear y ampliar su pipeline de talento

El primer paso para garantizar que dispone de los recursos que necesita es crear su pipeline de talento:

Contratación y prácticas de personas con estudios superiores

La colaboración con las universidades y escuelas técnicas locales puede proporcionarle un flujo constante de talento joven. Con la preparación adecuada, estas personas pueden convertirse en una parte valiosa del equipo pasado un tiempo.

Formación y desarrollo continuos

Aunque el tiempo y el presupuesto ejercen una presión constante, los profesionales de ciberseguridad deben estar al día de los cambios en las herramientas y las amenazas.

Priorización de la retención

Los buenos profesionales están muy solicitados, sobre todo si tienen experiencia en la gestión de ataques. Si no mantiene a sus mejores talentos, otra empresa lo hará.

Puede que un equipo sólido no sea suficiente para gestionar el estrés de un ataque, por lo que debe planificar con antelación e identificar asistencia adicional antes de que sea necesaria:

Evalúe los recursos de terceros

Las empresas de consultoría de ciberseguridad y ampliación de la plantilla pueden ayudar a su equipo durante las operaciones y los incidentes en curso. Establezca relaciones con esas organizaciones aunque no las necesite ahora para acceder a los recursos dado el momento.

Dell ofrece una serie de servicios que pueden aumentar los equipos, como CISO virtual (vCISO), respuesta ante incidentes y asesoría de ciberseguridad.

Saque provecho a AI

Aproveche las nuevas funciones de la IA integradas en las herramientas de ciberseguridad, como el análisis de registros, la detección de anomalías, el triaje de alertas de nivel bajo o la formación especializada, para satisfacer la falta de recursos y abordar las necesidades operativas al permitir que los miembros del equipo se centren en tareas prioritarias.

Las dificultades relacionadas con los recursos crecen durante un ciberataque

Como muestra la situación expuesta al principio, un ciberataque grave puede paralizar su organización al detener los sistemas y las operaciones empresariales principales. La empresa pierde dinero cada minuto que pasa, por lo que el equipo de ciberseguridad tendrá una enorme presión para solucionar el problema.

Garantizar que su personal esté lo más actualizado posible tendrá un impacto directo en la respuesta ante incidentes y el estrés relacionado con este.

La formación debe extenderse a todos los empleados, no solo a los profesionales de seguridad, ya que son la primera línea de defensa.

Esta historia destaca el principal reto: los ciberdefensores son, al fin y al cabo, humanos. Tienen límites, y cuando estos se superan, incluso los mejores profesionales pueden fallar. La fatiga mental, el estrés y el agotamiento son factores clave en el estado de ciberseguridad.

Aunque es posible que no haya una solución única para este reto, las siguientes estrategias pueden ser fundamentales:

Creación de un equipo y un pipeline de talento fuertes

La solución básica para este problema es no dejar que se convierta en una emergencia: crear un equipo férreo con redundancias.

Planificación del componente humano de un ataque

Los planes de respuesta ante incidentes son esenciales y deben incluir planes para administrar al personal, planificar y gestionar el tiempo de inactividad de los empleados.

Aprovechamiento de los recursos de terceros

Los consultores de ciberseguridad externos pueden ayudarle a ampliar su equipo. Los servicios de respuesta ante incidentes de Dell, por ejemplo, llevan a un equipo de expertos in situ en cuestión de horas para evaluar, contener e iniciar la corrección de inmediato. Hemos ayudado a muchos clientes a superar ciberataques.

La IA puede ser útil, pero no es la solución infalible

La IA es muy prometedora para la mejora de las herramientas y los programas de ciberseguridad. Sus funciones abarcarán desde el análisis predictivo hasta el desarrollo de programas de formación personalizados y la gestión proactiva de amenazas antes de que se propaguen.

Quizás la principal ventaja es que la IA proporciona a los defensores un sistema de asistencia en tiempo real durante un incidente. Los modelos de aprendizaje automático entrenados con datos históricos de ataque recomiendan acciones basadas en eventos anteriores similares.

A medida que el procesamiento de lenguaje natural se incorpora a las herramientas de ciberseguridad, los analistas tendrán la capacidad de interactuar directamente con sus sistemas, identificar amenazas e implementar soluciones.

La IA también puede supervisar los patrones de comportamiento para señalar cuándo un analista humano podría estar cometiendo errores repetidos (quizás debido al agotamiento) y recomendar un cambio de turno o una segunda opinión.

Aunque las herramientas de ciberseguridad integran rápidamente las herramientas de IA más sofisticadas, muchas de las funciones más potentes aún están en desarrollo. Tenga en cuenta que, en estos momentos, la IA no puede reemplazar las habilidades de un profesional experimentado, ***especialmente de uno que ya se ha enfrentado a un ataque***.

Recomendaciones para aprovechar la IA:

Comprender cómo las herramientas pueden contribuir a sus operaciones de seguridad

Lleve a cabo un análisis detallado de las herramientas de IA e impleméntelas donde puedan ser más eficaces. Entre las posibles ventajas están la detección de amenazas avanzadas, la automatización de tareas repetitivas y el uso de la IA en la gestión de identidades.

> Contar con un socio que se ocupe de la respuesta, la corrección y la recuperación de incidentes antes de que se produzcan es una práctica recomendada".
>
> ***Jason Rosselot***
> *Vicepresidente de ciberseguridad y director de seguridad de la unidad empresarial en Dell Technologies*

Planificar el futuro de la IA

Sepa cuándo estarán disponibles nuevas funciones y cómo beneficiarán a su equipo, y desarrolle un plan para implementarlas.

Incorporar la IA en la planificación de la plantilla

Dado que la automatización reduce las tareas manuales, es posible que la composición de su equipo de seguridad deba evolucionar. Quizás necesite recursos de nivel superior para analizar y actuar sobre la información de seguridad, en lugar de compilarla. Ajuste sus estrategias de contratación y desarrollo en consecuencia.

La IA se convertirá en una parte importante de sus operaciones de ciberseguridad, si todavía no lo ha hecho. Pero tenga en cuenta que nada puede sustituir a un profesional cualificado y experimentado. El objetivo debe ser utilizar la IA para automatizar las operaciones y hacer que los recursos humanos sean más eficaces, lo que, en última instancia, evita los ataques y minimiza su impacto cuando se producen.

Avances en la madurez de la ciberseguridad: paso a paso

Como cualquier aspecto de la ciberseguridad, gestionar el factor humano es un proceso, no un destino. El esfuerzo incremental e incluso los pequeños avances en el progreso marcan la diferencia y aumentan con el tiempo. Lo importante es recordar que incluso las mejores herramientas tecnológicas y de seguridad son, en última instancia, tan buenas como las personas que las utilizan.

DELL Technologies

Productos y soluciones Dell destacados

Solución Dell destacada	Descripción
Servicios de respuesta ante incidentes	Un equipo de expertos en ciberseguridad certificados está a su disposición para actuar rápidamente en caso de ciberataque. Colaboramos estrechamente con usted para acabar con las amenazas hasta que se reanuden las operaciones normales.
Cybersecurity Advisory Services	La orientación de expertos puede servirle para localizar y solucionar los puntos ciegos de su estrategia de seguridad, proteger sus activos y datos, y permitir una vigilancia y gobernanza continuas.
vCISO	Director de seguridad de la información virtual y experto en ciberseguridad que ayuda a identificar y gestionar riesgos, y guía la toma de decisiones estratégicas.
Managed Detection and Response	Reduce los esfuerzos manuales y optimiza las operaciones de seguridad diarias al proporcionar supervisión, detección de amenazas, investigación y respuesta rápida en puntos finales, redes y cloud. Los clientes eligen su plataforma XDR preferida (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR o Microsoft Defender XDR) y reciben orientación de expertos, informes trimestrales y hasta 40 horas anuales de respuesta ante incidentes.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**

DELL Technologies