CISCO
SECURE

5 maneras respaldadas por datos de lograr un impacto en la ciberseguridad

Los desafíos en materia de ciberseguridad no van a ninguna parte. Cada día, nuestro mundo está más conectado y se vuelve más complejo. Y, para los equipos de ciberseguridad, más complejidad equivale a más responsabilidad.

Afortunadamente, las empresas pueden tomar medidas concretas para mejorar los resultados en seguridad. En nuestro Estudio de Resultados de Seguridad, Vol. 2, recopilamos datos de más de 5100 profesionales de la seguridad y las telecomunicaciones de 27 países. A partir de esos datos, hemos identificado cinco prácticas clave que han demostrado impulsar el éxito de los programas de ciberseguridad. Aproveche la siguiente lista de comprobación:

Actualice su tecnología

El 39 % de las tecnologías de seguridad utilizadas por las organizaciones se consideran obsoletas.

No sea reactivo y evalúe su pila tecnológica después de un incidente. Cree hoy mismo una estrategia de actualización tecnológica más proactiva.

> Dado que casi el 40 % de las organizaciones tienen tecnologías de seguridad obsoletas, el problema de la deuda de seguridad es importante. Pero la buena noticia es que las organizaciones con modernas arquitecturas consolidadas en la nube logran un alto nivel de actualización tecnológica al ser proactivas en su estrategia tecnológica. Problema más solución" .
>
> Richard Archdeacon, Consejero de CISO, Cisco

Integre para mejorar la visibilidad

El 77 % de las organizaciones prefiere adquirir soluciones integradas que crearlas.

Afortunadamente, las soluciones basadas en la nube son cada vez más prominentes, de modo que las integraciones sólidas son más accesibles que nunca, lo que brinda a los equipos de seguridad una visibilidad más amplia de sus sistemas.

> La TI de seguridad moderna y bien integrada contribuye al éxito general del programa, más que cualquier otra práctica o control de seguridad" .
>
> Helen Patton, Consejera de CISO, Cisco

Amplíe su equipo

Las organizaciones con las proporciones de personal más altas tienen un 20 % más de probabilidades de contar con una detección de amenazas y una respuesta ante ellas más sólidas.

¿La ampliación del equipo no es una opción? Considere la posibilidad de mejorar las habilidades y competencias del personal existente. La formación es siempre una inversión inteligente.

> Elija a las personas más capacitadas para sus equipos de SecOps porque eso importa más que el número de personas. La automatización puede ayudarle a reducir la brecha con el personal de nivel inferior para obtener resultados tan sólidos como si tuviera más personal de nivel superior" .
>
> Wendy Nather, Consejera jefe de CISO, Cisco

Trabaje de manera más inteligente con la inteligencia de amenazas

Las organizaciones que utilizan la inteligencia de amenazas tienen el doble de probabilidades de informar sobre capacidades sólidas de detección y respuesta.

Tanto si el crecimiento del equipo es una opción como si no lo es, utilice todas las herramientas de inteligencia disponibles para salvar esa brecha. Trabaje de forma más inteligente para obtener resultados más sólidos.

> Cuando las empresas combinan personas, procesos y tecnologías potentes, logran capacidades avanzadas de detección de amenazas y respuesta a amenazas, cuando se completan con una sólida inteligencia de amenazas" .
>
> Dave Lewis, Consejero de CISO, Cisco

Rompa las cosas a propósito

Las empresas que se dedican a la ingeniería del caos tienen el doble de probabilidades de ver mejorada la continuidad del negocio.

La interrupción periódica e intencionada de las TI preparará a su organización para hacer frente a las amenazas reales. Abrace el caos para prepararse para el caos.

> Las organizaciones que realizan pruebas periódicas y variadas tienen 2,5 veces más probabilidades de mantener sus operaciones ante una emergencia. Esto se puede reforzar aún más siguiendo las prácticas de ingeniería del caos" .
>
> Wolfgang Goerlich, Consejero de CISO, Cisco

Seguir estos pasos respaldados por datos le pondrá en el camino hacia una postura en materia de ciberseguridad más sólida. Pero no se limite a creer en nuestra palabra. Para ver todos los datos que respaldan nuestros hallazgos, consulte el informe completo.

Obtener el informe

The bridge to possible