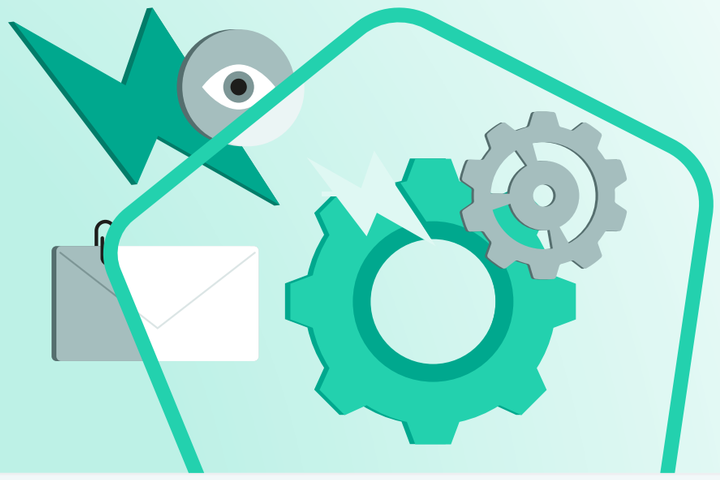
Mitos de la respuesta a incidentes

Demos un paso atrás y examinemos algunos de los mitos que rodean esta creciente área de preocupación por la seguridad empresarial.



Mito n.° 1

Cualquier arreglo es mejor que ningún arreglo

Mito También conocido como “no te quedes ahí parado, ¡haz algo!”. Este mito es parcialmente cierto, pero solo si suponemos que “cualquier arreglo” alcanza algún nivel de resolución. Pero analizar una alerta individual que se aproxima a cada incidente por partes es ineficaz. Demasiados equipos carecen de un enfoque sistemático general para la respuesta a incidentes y, por lo tanto, pierden la oportunidad de aprovechar al máximo su talento interno.

En lugar de **Forme un enfoque de ciberseguridad más holístico para que pueda responder de manera rápida y eficaz, sin sacrificar uno por el otro. Desarrolle un enfoque sistemático a más largo plazo para la respuesta integral a incidentes que tenga en cuenta el futuro, así como la amenaza presente inmediata.**

Mito n.° 2

La respuesta termina con la contención de amenazas

Mito También conocida como la trampa del pensamiento a corto plazo. La respuesta a incidentes, en el sentido más estricto, se ocupa de gestionar las secuelas de una infracción de seguridad, incluida la constante lucha contra incendios que arruina la vida de demasiados expertos en seguridad de TI. Desafortunadamente, el alcance de las “consecuencias” con frecuencia se subestima. Entre otras cosas, debe incluir una investigación más profunda, una línea de tiempo completa del incidente y una reconstrucción lógica.

En lugar de **No se apresure a volver una vez que haya reparado el daño resultante de un incidente; investigue más para desarrollar una comprensión más profunda de la causa raíz, de modo que se puedan prevenir incidentes similares en el futuro, con un mínimo de problemas.**

Mito n.° 3

El éxito se puede medir por el número de incidentes resueltos

Mito La seguridad de TI del siglo XXI es una actividad emocionante, de alto riesgo, llena de suspenso, con equipos de expertos responsables ante una variedad de partes interesadas, incluido el director ejecutivo, los accionistas y los organismos reguladores. También es un campo altamente complejo y de élite, por lo que no es de extrañar que los expertos en seguridad de TI, con frecuencia, midan la eficacia en términos de un “recuento de muertes” de incidentes cibernéticos.

En lugar de **Medir el valor de los procesos de respuesta a incidentes en términos de métricas de tiempo medio de detección y tiempo medio de respuesta (MTTD/MTTR) y tener en cuenta métricas más amplias, como el ahorro de costos y el nivel de daño evitado (tanto reputacional como operativo).**

Mito n.° 4

Incidentes Los servicios de respuesta son una propuesta de una u otra cosa

Mito En lugar de formular la pregunta de subcontratación de respuesta a incidentes, como “¿deberíamos hacerlo internamente O deberíamos contratar apoyo externo?”, considere optar por un enfoque combinado. Su equipo interno son los expertos más importantes en esta situación, y eso no cambia cuando contrata servicios externos de respuesta a incidentes.

En lugar de **Busque servicios de respuesta a incidentes que se sumen a los esfuerzos generales de su equipo interno. En este sentido, los servicios de TI deben entenderse como una de las muchas herramientas vitales que sus expertos pueden aprovechar para defenderse de incidentes complejos.**

Mito n.° 5

Si necesita servicios de respuesta a incidentes, debe estar haciendo algo mal

Mito Esto podría haber sido cierto para organizaciones de seguridad de TI desarrolladas muy grandes hace dos décadas, pero está lejos de ser cierto hoy, debido al complejo horizonte de amenazas, la necesidad de inteligencia de amenazas global y la necesidad de aprovechar el ecosistema de ciberseguridad más amplio.

En lugar de **Nutra el poder de la ciberseguridad de su equipo con tecnología líder en la industria que los coloca en una mejor posición para llevar a cabo sus propios procesos de respuesta a incidentes, al tiempo que refuerza aquellos con experiencia externa cuando sea necesario.**
