El checklist del CISO para prepararse ante Mythos

Las actualizaciones con los parches están al caer. Antes de que se implementen, tu consejo de administración, tu equipo jurídico y los reguladores tendrán preguntas.

1 Exposición y visibilidad de activos

«¿Cuál es nuestra exposición, y disponemos de un inventario de activos preciso?»

- [ ] Actualiza tu inventario de activos para que refleje tu entorno de producción actual.
- [ ] Confirma que el escaneo continuo está activo en todos los entornos de producción.
- [ ] Reclasifica las vulnerabilidades usando una priorización basada en el riesgo, no en el recuento bruto de CVE.
- [ ] Prepara un informe de una página sobre la exposición, para cuando lo solicite la dirección.

2 Velocidad de aplicación de parches y seguridad en la producción

«¿Podemos aplicar los parches con la suficiente rapidez, a escala, y sin interrumpir el servicio?»

- [ ] Audita la cadencia actual del ciclo de parches en relación con el margen de tiempo entre la divulgación y la explotación.
- [ ] Clasifica los activos por nivel de criticidad antes de que llegue la oleada, no durante la misma.
- [ ] Establece un protocolo de gestión de cambios con responsables designados y vías de reversión.
- [ ] Realiza un simulacro sobre un despliegue de parches de alta velocidad para poner a prueba las vías de decision y la preparación para la reversión.

3 Cadena de suministro y exposición al código abierto

«¿Qué se oculta en nuestro software de código abierto y de terceros?»

- [ ] Genera o actualiza tu lista de components de software (SBOM).
- [ ] Realiza un inventario de las integraciones de terceros heredadas a través de adquisiciones.
- [ ] Implanta el escaneo continuo de las dependencias de las bibliotecas de código abierto.
- [ ] Identifica los SLA de los proveedores en materia de parches y los puntos de contacto antes de que se haga pública la Información.

4 Capacidad de ingeniería

«¿Tenemos la capacidad de ingeniería para ponernos al día con nuestro propio trabajo pendiente?»

- [ ] Calcula las horas necesarias para ponerte al día en función de los compromisos actuales de tu equipo.
- [ ] Prioriza el backlog para que los equipos internos se centren solo en las tareas de mayor riesgo.
- [ ] Asegura recursos de ingeniería externos antes de que los necesites.
- [ ] Incorpora ya prácticas de "seguridad por defecto" en el desarrollo continuo.

5 Detección y contención

«Si un parche se retrasa, ¿podemos detectar y contener el exploit?»

- [ ] Asegúrate de que la supervision del SOC esté activa 24/7 en todos los entornos críticos.
- [ ] Define un tiempo medio objetivo para la clasificación y el asilamiento (en minutos, no en horas).
- [ ] Lleva a cabo búsquedas proactivas de amenazas centradas en las superficies de exposición de Mythos.
- [ ] Valida tu plan de actuación para el supuesto de una brecha mediante un ejercicio o simulación reciente.

Comprobación de preparación ejecutiva

Antes de informar a la dirección:

- [ ] Identifica cuáles de estas respuestas puedes defender hoy mismo y cuáles requieren el apoyo de la dirección o una justificación adicional.

Si estás decidiendo cómo cubrir estas carencias:

Algunas organizaciones desarrollan estas capacidades internamente; otras se asocian para acelerar la cobertura o reforzar a los equipos con recursos limitados.

Insight Managed Exposure Defence es un enfoque integrado que abarca las cinco áreas mencionadas anteriormente: primero se desarrolla y gestiona internamente, y luego se extiende a los clientes que se enfrentan a las mismas cuestiones.

Más información en es.insight.com