Cumplimiento y riesgo

Cómo afecta la prevención autónoma en el dispositivo a las obligaciones regulatorias, la notificación de infracciones, la soberanía de los datos, el seguro cibernético y la elaboración de informes de riesgo a nivel de junta directiva.

¿Cyber Crucible recopila claves de cifrado?

La respuesta más breve es: “No”.

Hubo un tiempo en que el software de Cyber Crucible no detenía el cifrado del ransomware antes de que ocurriera. En su lugar, recopilaba posibles claves de cifrado o configuraciones, y luego utilizaba una variedad de técnicas para determinar el paquete de descifrado adecuado (incluidas las claves) para descifrar después de un ataque de ransomware.

Desde el punto de vista de lo que recopilábamos, una buena analogía sería una cámara de video que tomara fotografías de todo lo que pudiera ser una clave para un casillero. Luego, un servidor realizaba los distintos cálculos matemáticos para determinar la clave y configuración adecuadas para el archivo correspondiente. Los científicos informáticos llamarían a esto aprendizaje automático.

Antes de dejar atrás el antiguo modelo de software de “recopilar todo lo que pudiera ser una clave”, organizábamos automáticamente miles de claves y configuraciones de cifrado por máquina durante los ataques.

El módulo de software de análisis criptográfico ha evolucionado ahora hacia un módulo analítico conductual adicional, que se utiliza como una fuente de datos para determinar si un software está intentando acceder de manera indebida a datos de identidad o “datos de datos” con el fin de robarlos o cifrarlos.

Si se previene un ataque, ¿aún tenemos que reportar una brecha?

Respuesta breve: Generalmente no. Cuando un ataque se detiene antes de su ejecución y no se accede, altera ni exfiltra ningún dato, típicamente no hay una brecha que divulgar. Las obligaciones de divulgación suelen activarse por el acceso no autorizado a datos protegidos, no por un intento que fracasó.

Un ejemplo real

En la implementación de servicios financieros donde Cyber Crucible interceptó casi 10,000 procesos maliciosos, el resultado para el CISO incluyó cero divulgación regulatoria. Debido a que los ataques se detuvieron antes de su ejecución y no se tocó ningún dato, no hubo notificaciones requeridas a clientes, proveedores o reguladores gubernamentales, ni titulares de noticias, lo que preservó la confianza del cliente.

Una advertencia importante

Los requisitos de divulgación varían según la jurisdicción, la industria y el contrato, y los hechos específicos de un incidente importan. Cyber Crucible no es un bufete de abogados y esto no constituye asesoramiento legal. El principio confiable es que la prevención reduce drásticamente su exposición a la divulgación en comparación con la detección posterior al hecho, pero su asesor legal y su equipo de cumplimiento deben tomar la determinación para cualquier evento en particular.

¿Cómo respalda Cyber Crucible el cumplimiento de la HIPAA en el sector sanitario?

Respuesta breve: Todo el análisis se realiza localmente a nivel del kernel, de modo que la información de salud protegida nunca sale del endpoint para su procesamiento de seguridad. Esto evita la exposición ante la HIPAA que generan las herramientas de seguridad que cargan archivos o claves sensibles a nubes de terceros, y detiene los ataques sin necesidad de desconectar los sistemas clínicos.

El problema de la seguridad alojada por el proveedor

Muchos acuerdos de SOC y MDR alojados por el proveedor requieren cargar claves, archivos o telemetría sensibles a bases de datos en la nube de terceros. Para una entidad cubierta, esto genera un riesgo real de cumplimiento y aumenta el número de partes que manejan datos protegidos.

Análisis local, datos locales

Cyber Crucible analiza en el endpoint. Los activos sensibles nunca salen del límite seguro del dispositivo, lo que respalda tanto la soberanía de los datos como la postura regulatoria asociada.

La continuidad importa clínicamente

La contención que requiere aislar una máquina o forzar un reinicio no es aceptable cuando la atención al paciente depende de ello. La suspensión selectiva únicamente del proceso malicioso significa que el ataque se neutraliza en menos de 200 milisegundos mientras las operaciones médicas, los dispositivos conectados y los sistemas clínicos siguen funcionando.

¿Cómo respalda Cyber Crucible el cumplimiento de FERPA y la privacidad de los datos de los estudiantes?

Respuesta breve: FortressAI verifica el acceso a los datos en el dispositivo, de modo que los registros estudiantiles y los datos familiares no puedan llegar accidentalmente a una herramienta de IA pública. Cyber Crucible detiene el ransomware de forma autónoma sin requerir un centro de operaciones de seguridad (SOC) las 24 horas del día, los 7 días de la semana, algo que la mayoría de los distritos e instituciones no pueden financiar.

Los dos problemas de la educación

Las escuelas y universidades son objetivos preferidos del ransomware, y rara vez cuentan con presupuesto para una dotación de personal de SOC permanente. Al mismo tiempo, la adopción de IA en el aula ha avanzado mucho más rápido que la gobernanza correspondiente.

Cómo se abordan ambos problemas

- **Ransomware sin un SOC:** la prevención autónoma a nivel de kernel detiene los ataques en menos de 200 milisegundos, sin necesidad de contratar analistas ni financiar un contrato de monitoreo 24/7.
- **Uso de IA alineado con FERPA:** FortressAI evalúa cada instrucción (prompt) en el dispositivo, de modo que los registros educativos protegidos y los datos personales familiares no terminen en un sistema de IA público, ni siquiera como datos de entrenamiento.

Esa combinación protege a los estudiantes y al personal sin agregar una carga significativa de trabajo de TI.

¿Qué significa la soberanía de datos para las implementaciones de Cyber Crucible?

Respuesta breve: Sus datos permanecen donde usted los coloque. El análisis y la aplicación de medidas ocurren en el endpoint, y Cyber Crucible puede implementarse completamente en las instalaciones (on-premises), operando en racks de servidores físicamente protegidos en lugar de una nube pública, sin plataformas de terceros, sin acceso externo y sin compartir datos.

Por qué los datos de seguridad centralizados son un riesgo

Las arquitecturas de seguridad que centralizan material sensible —claves de cifrado, tokens de sesión, datos de identidad— crean un único punto de falla y un objetivo de alto valor tanto para atacantes criminales como para aquellos patrocinados por estados.

Existe un segundo riesgo que recibe menos atención: un gobierno podría exigir acceso a datos almacenados de forma centralizada mediante una citación clasificada o una carta de seguridad nacional, sin el conocimiento ni el consentimiento del cliente. Se trata de una exposición profunda en materia de soberanía de datos, sin transparencia alguna.

La opción on-premises

Para las organizaciones que requieren un control absoluto, Cyber Crucible ofrece una instalación completamente on-premises, incluida la implementación con espacio de aire (air-gapped) y una arquitectura multiinquilino (multi-tenant) adecuada para gestionar múltiples departamentos o agencias desde una única instancia segura.

¿Qué riesgo de cumplimiento genera el depósito en custodia de claves de cifrado (key escrow), y por qué Cyber Crucible no lo hace?

Respuesta breve: Almacenar claves de cifrado de forma centralizada crea un punto único de falla, un objetivo de alto valor y exposición a la divulgación obligatoria. El enfoque de prevención de Cyber Crucible no depende de capturar o depositar en custodia las claves, por lo que no existe un almacén central de claves que asegurar, que sea objeto de una citación judicial o que pueda vulnerarse.

> Para la respuesta directa sobre el producto, consulte el artículo existente **"¿Cyber Crucible recopila claves de cifrado?"**. Esta página aborda el razonamiento de cumplimiento y soberanía de datos detrás de esa respuesta.

Por qué esto es deliberado

Cyber Crucible originalmente desarrolló y patentó tecnología de captura de claves para la defensa contra ransomware. Para 2021, las variantes de ransomware habían evolucionado para derrotarla, utilizando bibliotecas de cifrado personalizadas, implementaciones únicas por ejecución y cifrados de flujo (streaming ciphers) inmunes a la captura de claves. Presentamos ese criptoanálisis públicamente en BSides Pittsburgh en 2021.

El riesgo que decidimos no crear

Además de haber dejado de funcionar, la captura de claves requiere el almacenamiento centralizado de claves de cifrado. Eso introduce un punto único de falla, un objetivo de alto valor y la posibilidad de divulgación obligatoria sin conocimiento del cliente.

Prevenir el ataque antes de que comience el cifrado elimina por completo la necesidad de claves, lo cual constituye tanto una defensa más sólida como una superficie de cumplimiento más reducida.

¿Cómo afecta la prevención autónoma al seguro cibernético y a los informes ante la junta directiva?

Respuesta breve: La prevención cambia lo que usted reporta. En lugar de documentar incidentes, tiempos de inactividad y costos de remediación, usted reporta ataques que fueron detenidos sin interrupción del negocio, sin divulgación y sin pago de rescate.

Lo que realmente le importa a la junta directiva

En la implementación de servicios financieros referenciada a lo largo de esta base de conocimientos, el CISO pudo reportar cuatro resultados:

- **Cero paralización del negocio** — los ataques se suspendieron en memoria; las operaciones y las transacciones legítimas continuaron.
- **Cero divulgación regulatoria** — nada fue accedido, por lo que nada requirió notificación.
- **Cero daño de relaciones públicas** — sin titulares, se preservó la confianza del cliente.
- **Fuerte retorno de inversión** — una fracción del costo de la pila de tecnología heredada logró el trabajo que dicha pila no detectó.

Sobre los pagos de rescate

Aproximadamente el 90% de las víctimas de ransomware pagaron el rescate en 2023. Los clientes de Cyber Crucible no pagaron nada, porque los ataques no llegaron a la etapa de cifrado.

Para las aseguradoras

Los suscriptores preguntan cada vez más qué controles previenen un incidente en lugar de qué herramientas detectan uno. Un control autónomo a nivel de kernel que opera sin tiempo de

respuesta humana es una respuesta sustantiva — aunque los términos de cobertura siempre los establece su aseguradora.