Programa y Operaciones de Seguridad

Cómo Cyber Crucible opera su programa de seguridad — gestión de cambios, gestión de parches y vulnerabilidades, recuperación ante desastres y continuidad del negocio, respuesta a incidentes y violaciones de datos, y control de endpoints — descrito para revisores de riesgo de proveedores. Establece claramente qué está documentado y qué se proporciona bajo NDA, y no reclama ninguna certificación.

¿Cyber Crucible cuenta con un proceso de gestión de cambios?

Respuesta breve: Sí. Los cambios en producción siguen un proceso documentado de gestión de cambios que incluye revisión, pruebas y aprobación. Dado que el producto opera a nivel de kernel, la disciplina de cambios se trata como un control de seguridad y no simplemente como una práctica de ingeniería.

Qué abarca el proceso

Los cambios al código de la aplicación, los controladores de kernel, las configuraciones de servidor y la infraestructura de soporte pasan por etapas definidas del ciclo de vida: los requisitos de seguridad se establecen en la fase de diseño; el código fuente está controlado por versiones y los secretos nunca se incorporan en texto claro; las pruebas automatizadas validan los cambios antes de su promoción; y los cambios en producción reciben una revisión y aprobación formales. Se mantiene la segregación de funciones, de modo que el autor de un cambio no es su único aprobador. Las configuraciones base de los servidores siguen guías de configuración aprobadas, y los servicios no utilizados se deshabilitan cuando es posible.

Cambios de emergencia y de controladores

Los cambios de emergencia utilizan una vía expedita que, no obstante, sigue requiriendo autorización, pruebas específicas y una revisión posterior a la implementación. Los controladores de kernel de Windows se someten a controles internos de calidad y se envían para obtener la certificación del Programa de Compatibilidad de Hardware de Windows (WHCP) de Microsoft antes de su publicación, una verificación externa e independiente del componente con mayores privilegios.

Alineación con marcos de referencia y el límite honesto

El proceso se alinea con NIST SP 800-53 (familia CM) y con ISO/IEC 27001:2022 A.8.32. Cyber Crucible no reclama certificación alguna. El procedimiento detallado de gestión de cambios y la

evidencia de respaldo se proporcionan a los evaluadores bajo un acuerdo de confidencialidad (NDA).

¿Cuenta Cyber Crucible con un programa de gestión de parches?

Respuesta breve: Sí. Un programa de gestión de parches y vulnerabilidades basado en riesgos mantiene actualizados el software, los controladores del kernel, los servidores y los endpoints, y los hallazgos se rastrean hasta su resolución.

Cómo funciona

Se ejecutan pruebas de seguridad automatizadas continuas dentro del pipeline de desarrollo, se realizan pruebas de penetración manuales basadas en riesgos con un mínimo anual, y se ejecutan pruebas activadas por eventos con cada cambio significativo, abarcando tanto las redes internas como externas. Los parches de seguridad y las correcciones urgentes (hot-fixes) se aplican según la recomendación del proveedor, y los grupos responsables tienen la obligación de mantenerse al día con los parches aplicables. Los medios extraíbles y portátiles se someten a la misma protección y análisis que los medios fijos.

Priorización e implementación

Los hallazgos se priorizan según su gravedad y explotabilidad, y las vulnerabilidades activamente explotadas se gestionan mediante una vía expedita fuera de banda. Los parches siguen el proceso de gestión de cambios —validados antes de su promoción a producción— y las actualizaciones de controladores del kernel se revalidan mediante Microsoft WHCP antes de su publicación.

Alineación con marcos de referencia y el límite honesto

El programa se alinea con NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 e ISO/IEC 27001:2022 A.8.8. No se reclama ninguna certificación. Los plazos de remediación objetivo específicos y la evidencia de remediación se proporcionan a los evaluadores bajo un acuerdo de confidencialidad (NDA).

¿Cuenta Cyber Crucible con un plan de recuperación ante desastres y continuidad del negocio?

Respuesta breve: Sí. Cyber Crucible mantiene un plan de recuperación ante desastres probado, a cargo de la dirección de TI, y una arquitectura diseñada para alta disponibilidad. Dado que la prevención de amenazas se ejecuta localmente en el endpoint, la protección del endpoint continúa incluso durante una interrupción del backend de gestión.

Resiliencia por diseño arquitectónico

El backend de gestión está construido con almacenamiento redundante y replicado, de modo que la pérdida de un nodo individual no provoca pérdida de datos ni tiempo de inactividad. El Acuerdo de Nivel de Servicio publicado establece un compromiso de disponibilidad mensual del 99.9% para el backend de gestión y generación de informes, excluyendo el mantenimiento programado y las causas fuera de un control razonable. La protección del endpoint en sí no se ve afectada por una interrupción del backend.

Copias de seguridad y planificación de contingencia

Los datos se replican y respaldan continuamente en almacenamiento externo seguro utilizando credenciales privilegiadas distintas, con copias de seguridad protegidas contra ransomware mediante manejo fuera de línea o inmutable, y se prueban de manera periódica. El plan mantiene un plan de respuesta a emergencias informáticas, un plan de sucesión, un estudio de criticidad de datos y una lista de criticidad de servicios, e incorpora un análisis de impacto en el negocio, estrategias de recuperación, un plan de comunicación que incluye la notificación a los clientes, y objetivos de recuperación definidos. Las pruebas incluyen ejercicios de simulación (table-top) y simulacros de recuperación.

Alineación con marcos de referencia y el límite honesto

El plan se alinea con NIST SP 800-34 e ISO/IEC 27001:2022 A.5.29–A.5.30. Cyber Crucible define objetivos de punto de recuperación y de tiempo de recuperación para el backend; los valores objetivo específicos, así como el plan en sí, se proporcionan a los revisores bajo un acuerdo de confidencialidad (NDA). Dado que la protección se ejecuta localmente, la defensa del endpoint continúa sin una brecha significativa en el tiempo de recuperación durante una interrupción del backend o en un despliegue con air-gap.

¿Cuenta Cyber Crucible con un proceso de respuesta a incidentes y notificación de brechas?

Respuesta breve: Sí. Un proceso documentado de respuesta a brechas de datos define los roles y pasos para responder ante un presunto robo, brecha o exposición de datos protegidos, incluida la notificación al cliente. Se puede establecer contractualmente un plazo de notificación comprometido para clientes regulados.

El proceso de respuesta

Un presunto incidente se reporta de inmediato a través de canales internos supervisados por la función de Seguridad de la Información. Al identificarse, se elimina el acceso al recurso afectado y se convoca un equipo de respuesta a incidentes presidido por la alta dirección ejecutiva. Los investigadores y expertos forenses, proporcionados a través del seguro cibernético y tecnológico de Cyber Crucible, determinan cómo ocurrió el incidente, los datos involucrados, las partes afectadas y la causa raíz. Se desarrolla un plan de comunicación junto con los departamentos Legal, de Comunicaciones y de Recursos Humanos para notificar al personal, al público y a las partes afectadas según corresponda —incluida la notificación al cliente a través de un canal mutuamente acordado—, seguido de una revisión posterior al incidente.

Respuesta de soporte y notificación

Los incidentes orientados al cliente se rastrean conforme a los niveles de gravedad publicados en el SLA (SEV1 a SEV4), y se puede comprometer contractualmente un plazo de notificación de brechas o incidentes para clientes regulados.

Alineación con marcos de referencia y el límite honesto

El proceso se alinea con NIST SP 800-61 e ISO/IEC 27001:2022 A.5.24–A.5.26. No se reclama ninguna certificación. El procedimiento completo de respuesta a incidentes y notificación de brechas se proporciona a los revisores bajo NDA.

¿Cómo protege y controla Cyber Crucible los endpoints?

Respuesta breve: De dos maneras. El producto en sí es una prevención autónoma de endpoints que opera en la capa del kernel, y Cyber Crucible controla sus propios endpoints corporativos y de ingeniería bajo un programa formal. Ambos se apoyan en el desarrollo interno del código con mayores privilegios.

Protección de endpoints del producto

El producto ofrece prevención autónoma contra ransomware, ataques en memoria (fileless) e inyección de procesos, aplicada en la capa del kernel. Está deliberadamente desacoplado de las bibliotecas del sistema operativo, de modo que cuando los atacantes comprometen o secuestran esas bibliotecas en memoria, el producto continúa ejecutándose, aplicando controles e informando. Debido a que la detección y respuesta se ejecutan localmente, la protección continúa durante una interrupción del backend de gestión o en una implementación deliberadamente aislada (air-gapped).

Integridad de la cadena de suministro y validación independiente

Los algoritmos de detección, las heurísticas del kernel, los sensores y los controladores se diseñan y mantienen internamente; no se integran en el software bibliotecas de terceros no verificadas ni ganchos de telemetría ocultos. Debido a que el componente con mayores privilegios es propietario, se elimina por completo una categoría de exposición de la cadena de suministro de terceros, en lugar de simplemente gestionarla. Todos los controladores de kernel de Windows se validan y firman bajo el Programa de Compatibilidad de Hardware de Windows (WHCP) de Microsoft.

Controles de endpoints corporativos

Los endpoints gestionados siguen líneas de base de configuración segura aprobadas, ejecutan protección y análisis de endpoints, y aplican los mismos controles a los medios extraíbles y portátiles que a los medios fijos, restringiendo el uso no autorizado de medios. La instalación de software se rige por políticas, los datos en reposo en los endpoints se cifran, y los endpoints se

mantienen actualizados conforme al programa de gestión de parches.

Alineación con marcos de referencia y el límite honesto

Los controles de endpoints se alinean con los Controles Críticos de Seguridad del CIS (v8) y el NIST SP 800-53 (SI-3, CM-2, MP-7). No se reclama ninguna certificación. Se proporcionan estándares de configuración detallados y evidencia a los revisores bajo un acuerdo de confidencialidad (NDA).

¿Qué políticas de seguridad mantiene Cyber Crucible y cómo puedo solicitarlas?

Respuesta breve: Cyber Crucible mantiene un conjunto completo de políticas de seguridad de la información, que abarca uso aceptable, acceso y autenticación, cifrado, gestión de cambios, recuperación ante desastres, respuesta a incidentes y brechas, retención y destrucción de datos, entre otras. Las políticas y la evidencia de respaldo están disponibles para los revisores bajo acuerdo de confidencialidad (NDA).

Áreas de política representativas

El conjunto de políticas abarca uso aceptable y ética; acceso, autenticación y acceso remoto; cifrado y protección de claves; desarrollo seguro y gestión de cambios; seguridad de servidores y endpoints; recuperación ante desastres y continuidad del negocio; respuesta a incidentes y brechas; y retención de datos, destrucción y retención de correo electrónico. Los resúmenes de programas para cumplimiento, auditoría y gobernanza de IA/SDLC se mantienen junto con las políticas.

Qué es público y qué está bajo NDA

Las páginas públicas de la base de conocimientos describen la existencia, los principios y la alineación con los marcos de referencia de cada programa, de modo que un revisor pueda comprender la postura a un nivel general. Los documentos de políticas específicos, los estándares de configuración, las cifras exactas (como los cronogramas de retención y los objetivos de recuperación) y la evidencia de auditoría son confidenciales y se proporcionan bajo un NDA mutuo, junto con el paquete preparado de debida diligencia para proveedores.

Cómo solicitarlas

Los revisores pueden solicitar el conjunto de políticas de seguridad, el paquete preparado para proveedores y la evidencia de respaldo a **dpo@cybercrucible.com**. El NDA mutuo estándar de Cyber Crucible está disponible en caso de que no se cuente ya con uno. No se reclama certificación para ningún marco de referencia; la documentación explica cómo la arquitectura y los controles respaldan cada obligación.