

¿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).

Revision #1

Created 2026-07-24 23:16:24 UTC by Dennis Underwood

Updated 2026-07-24 23:16:24 UTC by Dennis Underwood