Cyber Crucible dispose-t-il d'un programme de gestion des correctifs ?

Réponse courte : Oui. Un programme de gestion des correctifs et des vulnérabilités fondé sur les risques permet de maintenir à jour les logiciels, les pilotes de noyau, les serveurs et les postes de travail, et les constats sont suivis jusqu'à leur résolution.

Fonctionnement

Des tests de sécurité automatisés continus s'exécutent au sein du pipeline de développement, des tests d'intrusion manuels fondés sur les risques sont réalisés avec un minimum annuel, et des tests déclenchés par événement sont exécutés à chaque modification significative, couvrant à la fois les réseaux internes et externes. Les correctifs de sécurité et les correctifs à chaud sont appliqués conformément aux recommandations des fournisseurs, et les groupes propriétaires sont responsables de rester à jour sur les correctifs applicables. Les supports amovibles et portables sont soumis à la même protection et au même contrôle par analyse que les supports fixes.

Priorisation et déploiement

Les constats sont priorisés selon la gravité et l'exploitabilité, les vulnérabilités activement exploitées étant traitées via un parcours accéléré, hors bande. Les correctifs suivent le processus de gestion des changements — validés avant leur passage en production — et les mises à jour des pilotes de noyau sont revalidées via Microsoft WHCP avant leur publication.

Alignement avec les référentiels et limite de transparence

Le programme s'aligne sur les normes NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 et ISO/IEC 27001:2022 A.8.8. Aucune certification n'est revendiquée. Les délais de remédiation cibles spécifiques et les preuves de remédiation sont fournis aux évaluateurs sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 23:43:37 UTC by Dennis Underwood
Updated 2026-07-24 23:43:37 UTC by Dennis Underwood