A Cyber Crucible possui um programa de gestão de patches?

Resposta curta: Sim. Um programa de gestão de patches e vulnerabilidades baseado em risco mantém softwares, drivers de kernel, servidores e endpoints atualizados, e as constatações são acompanhadas até sua resolução.

Como funciona

Testes de segurança automatizados contínuos são executados no pipeline de desenvolvimento, testes de penetração manuais baseados em risco são realizados com um piso anual, e testes acionados por eventos são executados a cada alteração significativa, cobrindo tanto redes internas quanto externas. Patches de segurança e hot-fixes são aplicados conforme recomendação do fornecedor, e os grupos responsáveis devem manter-se atualizados quanto aos patches aplicáveis. Mídias removíveis e portáteis são submetidas ao mesmo nível de proteção e verificação que as mídias fixas.

Priorização e implantação

As constatações são priorizadas por severidade e explorabilidade, com vulnerabilidades ativamente exploradas tratadas por meio de um caminho expedito e fora de banda. Os patches seguem o processo de gestão de mudanças — validados antes da promoção para produção — e as atualizações de drivers de kernel são revalidadas por meio do Microsoft WHCP antes do lançamento.

Alinhamento a frameworks e o limite honesto

O programa está alinhado ao NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 e ISO/IEC 27001:2022 A.8.8. Nenhuma certificação é reivindicada. Janelas específicas de remediação-alvo e evidências de remediação são fornecidas aos avaliadores sob NDA.

Revision #1
Created 2026-07-24 23:36:57 UTC by Dennis Underwood
Updated 2026-07-24 23:36:57 UTC by Dennis Underwood