Como a Cyber Crucible protege e controla os endpoints?

Resposta curta: De duas formas. O próprio produto é uma prevenção autônoma de endpoints que opera na camada de kernel, e a Cyber Crucible controla seus próprios endpoints corporativos e de engenharia sob um programa formal. Ambos se baseiam na construção interna do código com maior nível de privilégio.

Proteção de endpoints do produto

O produto oferece prevenção autônoma contra ransomware, ataques em memória (fileless) e injeção de processos, aplicada na camada de kernel. Ele é deliberadamente desacoplado das bibliotecas do sistema operacional, de modo que, quando invasores comprometem ou sequestram essas bibliotecas em memória, o produto continua a executar, aplicar controles e reportar. Como a detecção e a resposta são executadas localmente, a proteção continua durante uma interrupção do back-end de gerenciamento ou em uma implantação deliberadamente isolada (air-gapped).

Integridade da cadeia de suprimentos e validação independente

Os algoritmos de descoberta, heurísticas de kernel, sensores e drivers são projetados e mantidos internamente; nenhuma biblioteca de terceiros não verificada ou gancho de telemetria oculto é incorporado ao software. Como o componente de mais alto privilégio é proprietário, uma classe inteira de exposição da cadeia de suprimentos de terceiros é eliminada, e não apenas gerenciada. Todos os drivers de kernel do Windows são validados e assinados sob o Windows Hardware Compatibility Program (WHCP) da Microsoft.

Controles de endpoints corporativos

Os endpoints gerenciados seguem linhas de base de configuração segura aprovadas, executam proteção e varredura de endpoints, e aplicam os mesmos controles a mídias removíveis e portáteis que a mídias fixas, com o uso não autorizado de mídias restrito. A instalação de software é regida por política, os dados em repouso nos endpoints são criptografados, e os endpoints são mantidos atualizados sob o programa de gerenciamento de patches.

Alinhamento com frameworks e o limite honesto

Os controles de endpoints estão alinhados aos CIS Critical Security Controls (v8) e ao NIST SP 800-53 (SI-3, CM-2, MP-7). Nenhuma certificação é reivindicada. Padrões de configuração detalhados e evidências são fornecidos a revisores sob NDA.

Revision #1
Created 2026-07-24 23:37:27 UTC by Dennis Underwood
Updated 2026-07-24 23:37:27 UTC by Dennis Underwood