O que acontece se um dos meus produtos de segurança tiver um conflito com o Cyber Crucible?

Atualmente, o Cyber Crucible coexiste com todos os principais fornecedores de segurança, se utilizarmos os relatórios Magic Quadrant da Gartner como métrica dos incumbentes do setor.

O software de endpoint do Cyber Crucible é comprovadamente mais resiliente do que outros softwares, incluindo outras ferramentas de segurança de endpoint. Além disso, o outro software de segurança normalmente nem sequer tem visibilidade total sobre o software do Cyber Crucible.

Outra ferramenta de segurança tenta desativar o Cyber Crucible

Resumo:

A outra ferramenta tenta desativar parte do Cyber Crucible. Elas não conseguem. A ferramenta do outro fornecedor não testou o que acontece quando outra ferramenta (ou seja, o Cyber Crucible) diz: “não, eu não vou desativar”. As outras ferramentas travam ou entram em estado de erro.

Resposta do Cyber Crucible:

A resposta pode ser dupla. A primeira é incluir o software do Cyber Crucible na lista de permissões (whitelist) do outro fornecedor. Isso fará com que a outra ferramenta ignore o software do Cyber Crucible, o que (esperamos) evitará que a outra ferramenta entre em estado de erro.

Se isso não funcionar, cabe à nossa equipe encontrar uma solução. Aprendemos que outros fornecedores se movem muito mais lentamente (vários meses ou nunca) para corrigir um bug da parte deles.

Historicamente, nas poucas vezes em que isso aconteceu, basicamente criamos um ambiente em que a outra ferramenta acredita ter tido sucesso. Uma analogia não técnica seria deixar um familiar jovem ou uma criança vencer você em um jogo de damas.

Outra ferramenta de segurança tenta executar código se passando pelo Cyber Crucible

Resumo:

Isso ocorre muito raramente, mas já houve casos em que uma ferramenta de segurança tenta injetar seu código no programa em execução do Cyber Crucible e executar código se passando por nós.

Isso não é diferente de um hacker se passando por uma ferramenta de segurança, e não há como diferenciar se um hacker assumiu o controle do programa de segurança “confiável” (ou qualquer outro programa).

Resposta do Cyber Crucible:

Não existe cenário em que o Cyber Crucible permitirá que outra empresa (ou hacker) execute código se passando pelo nosso produto. A única solução, neste ponto, seria incluir o software do Cyber Crucible na lista de permissões (whitelist) da ferramenta do outro fornecedor. Não há mitigação que o Cyber Crucible possa fornecer para impedir que a outra ferramenta tente esse comportamento.

Felizmente, este é um evento muito raro.

O Cyber Crucible é desativado por outra ferramenta

Houve vários casos em que ferramentas de segurança com acessos altamente privilegiados tentavam repetidamente desativar o software do Cyber Crucible. Isso incluiu tentativas repetidas

de remover nosso driver ou encerrar nosso serviço continuamente.

Embora essas questões nunca tenham afetado a defesa contra extorsão, elas impactaram negativamente a experiência do usuário e o desempenho do sistema.

Tudo isso é histórico.

Se outra ferramenta tiver a capacidade, legítima ou não, de interromper o Cyber Crucible, um hacker também poderia ter essa capacidade.

Se você suspeitar ou observar que o software do Cyber Crucible foi diminuído de qualquer forma, independentemente do software que causou isso, entre em contato conosco imediatamente.

Normalmente, somos a última ferramenta de defesa entre um extorsionário e seus dados críticos. Não há espaço para fraquezas nessa circunstância.

Revision #1
Created 2026-07-24 05:44:15 UTC by Dennis Underwood
Updated 2026-07-24 05:44:15 UTC by Dennis Underwood