

A Cyber Crucible apresenta falsos positivos? Qual é a taxa de falsos positivos?

A Cyber Crucible busca proporcionar um ambiente de produto com 0 falsos positivos. Dito isso, às vezes ocorrem falsos positivos. Vamos discutir de onde eles vêm.

Atualmente, a taxa de falsos positivos é de aproximadamente 1 resposta por mês, a cada 1800 implantações/agentes, com total responsabilização sobre o motivo pelo qual essas respostas ocorrem.

Programa Corrompido Realizando Operações Rápidas em Arquivos

Seja de propósito ou por má programação, às vezes os programas se corrompem sozinhos, ou são corrompidos por outros programas durante a execução. Vemos isso com frequência em novos recursos de grandes suítes de programas, como o Microsoft Office, ou softwares proprietários personalizados.

O que acontece é que a memória do programa é corrompida, o que aumenta o nível de inspeção sobre o programa. Se isso for seguido por um comportamento de acesso a arquivos semelhante à extorsão, a Cyber Crucible é forçada a suspender o programa. Estamos melhorando na identificação de bugs conhecidos, e você consegue pelo menos continuar executando seu programa até que ele trave (alguns reiniciam automaticamente, outros não).

Em um mundo onde os invasores não usam o sistema de arquivos e, em vez disso, sequestram a memória de programas em execução, precisamos ser cautelosos.

A Cyber Crucible agora tem a capacidade de criar uma permissão, na qual, se o Programa A, com os Argumentos A, causar uma corrupção no Programa B, com os Argumentos B - podemos criar uma exclusão temporária para:

(Programa A + Argumentos A) abre (Programa B + Argumentos B)

Dessa forma, não se assume um risco adicional de que um hacker esteja envolvido, a menos que ele, por acaso, use exatamente os mesmos argumentos.

Um excelente exemplo disso ocorreu quando a Microsoft introduziu pela primeira vez a abertura de documentos do Office diretamente a partir de seu software de chat para desktop. Isso corrompia o programa Office... toda... única... vez... e então o programa Office começava a escanear todos os Documentos na máquina cerca de 25% das vezes. Isso... precisou de uma exclusão.

Se você tiver uma falha, use o botão de suporte, e ajudaremos você a criar uma exclusão, até que o fornecedor corrija o problema.

Programas de Segurança

A Cyber Crucible coexiste muito bem com programas de segurança. Ao contrário do que a maioria dos novos clientes pensa, ferramentas de segurança mais avançadas tendem a usar interações de sistema mais avançadas do que os programas antivírus que utilizam tecnologias mais antigas. De fato, algumas ferramentas de segurança gratuitas ou de baixo custo executam uma variedade de scripts inseguros do Powershell como parte fundamental de sua proteção, em vez de programas reais.

Como uma ferramenta de segurança altamente resiliente baseada em kernel, a Cyber Crucible é melhor compreendida como estando “mais abaixo”, ou “mais próxima” do hardware do que a maioria das outras ferramentas. A Cyber Crucible identifica e adiciona automaticamente outras ferramentas de segurança aos modelos comportamentais. Desde que as ferramentas de segurança não apresentem sinais de comprometimento, elas podem operar normalmente.

Ocasionalmente, uma ferramenta de segurança causa instabilidade no sistema quando suas tentativas de desativar ou interferir no software da Cyber Crucible falham. Nesses casos, o ideal é colocar a Cyber Crucible na lista de permissões da outra ferramenta de segurança, para impedir que ela tente (e falhe) desativar ou interferir na Cyber Crucible.

Sinta-se à vontade para abrir um chamado de suporte junto à Cyber Crucible, por meio do portal web, para discutir o assunto.

Ferramentas Administrativas ou de Backup

Em algumas circunstâncias, é necessário criar um comportamento personalizado para uma ferramenta administrativa ou de backup, enquanto a equipe da Cyber Crucible desenvolve um

modelo comportamental aprimorado. Nesse caso, a equipe da Cyber Crucible ajudará na criação de uma exceção no modelo comportamental, que isolará o programa mais os argumentos para uma janela de oportunidade extremamente pequena para um possível ataque.

Revision #1

Created 2026-07-24 05:51:58 UTC by Dennis Underwood

Updated 2026-07-24 05:51:58 UTC by Dennis Underwood