

Arquitetura e Tecnologia

Como o Cyber Crucible funciona nos bastidores - IA Genética, operação em nível de kernel, Rogue Process Prevention, independência do sistema operacional e por que as decisões são tomadas no endpoint.

- [Por que vocês respondem suspendendo programas?](#)
- [A Cyber Crucible impede toda a injeção de processo?](#)
- [O que são esses arquivos estranhos e de aparência aleatória que vejo?](#)
- [O que há de especial nos arquivos-canário da Cyber Crucible?](#)
- [Onde existem os arquivos canário?](#)
- [Como a Cyber Crucible utiliza a análise de memória?](#)
- [Como a Análise Comportamental de Memória da CC difere da varredura de memória?](#)
- [O Que Acontece Quando a CC Detecta Ataques de Memória](#)
- [O que é a IA Genética e em que difere de um LLM?](#)
- [Como o Cyber Crucible toma uma decisão em menos de 200 milissegundos?](#)
- [O que é a Rogue Process Prevention \(RPP\)?](#)
- [Que papel a análise de memória desempenha em toda a plataforma?](#)
- [Por que a Cyber Crucible opera no nível do kernel?](#)
- [O que significa o facto de a Cyber Crucible ser independente das bibliotecas do Windows?](#)
- [A Cyber Crucible funciona offline ou em ambientes isolados \(air-gapped\)?](#)
- [Por que a Cyber Crucible responde suspendendo um processo em vez de desligar o sistema?](#)

Por que vocês respondem suspendendo programas?

Os criminosos aprenderam que operar apenas em memória, utilizando técnicas como a injeção de processos, oferece uma variedade de vantagens:

1. Assumir o controle da identidade de um usuário para esse programa.
2. Evasão de verificações de gerenciamento de identidade.
3. Evasão de regras de firewall baseadas em aplicativos e listas de permissões.
4. Evasão de ferramentas de prevenção de perda de dados em servidores.
5. Eliminação de quase todas as evidências em memória quando o processo é encerrado.
6. Eliminação de quase todas as evidências em memória quando o computador é reiniciado.

Ao suspender os programas sob controle do invasor, as evidências ficam congeladas no tempo.

O invasor também fica congelado.

As evidências ficam disponíveis para ferramentas forenses como parte de um processo de investigação.

Se a organização não estiver equipada para realizar a perícia forense no momento, uma simples reinicialização por parte do invasor fará com que o sistema retorne a um estado saudável. Forçar o encerramento do programa suspenso e reiniciá-lo geralmente também produz o efeito desejado.

A Cyber Crucible impede toda a injeção de processo?

Não!

Existe uma variedade de atividades que ocorrem nos sistemas que constituem injeção de processo, mas que não são necessariamente maliciosas.

A Cyber Crucible torna todas essas atividades de injeção de processo visíveis para a caça a ameaças e análise de causa raiz, mas não interrompe a atividade a menos que as atividades de extorsão de dados, como roubo de dados ou criptografia por ransomware, sejam iniciadas.

Abaixo está um exemplo de injeção de processo realizada pelo software de segurança de endpoint da PC Matic, chamado PCPitStop. É provável que seja um comportamento que eles realizam para inspecionar os processos em execução.

5373968.png?width=680

Devido à análise comportamental em nível de kernel da Cyber Crucible, você tem visibilidade completa de todas as atividades, independentemente do nível de permissão do software (incluindo software altamente privilegiado da Microsoft ou de fornecedores de antivírus).

Se uma resposta automatizada for realizada, esta página e a página de Criações de Processos podem ser pesquisadas para fornecer resultados de investigação rápidos.

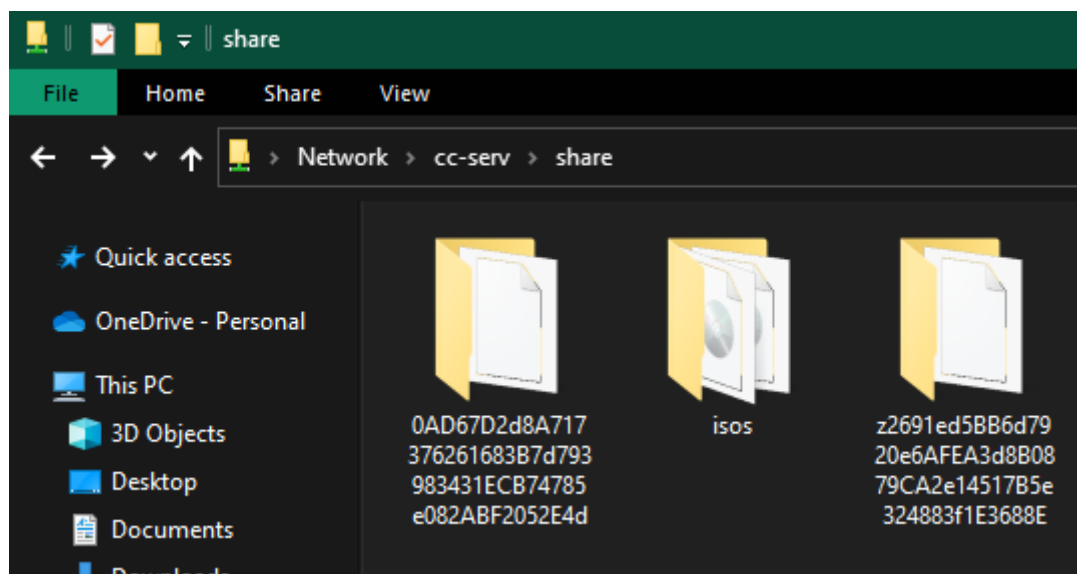
Além disso, a API REST pode ser utilizada pelas equipes de caça a ameaças para pesquisar indicadores de possíveis táticas maliciosas em memória.

O que são esses arquivos estranhos e de aparência aleatória que vejo?

O nosso software de Prevenção de Extorsão de Dados recebe indicadores comportamentais de vários mecanismos antes de tomar, em frações de segundo, a decisão sobre se um ataque está em curso. Um desses mecanismos, o mecanismo de monitorização de arquivos, utiliza arquivos especiais em vários locais.

Esses arquivos que por vezes vê, e por vezes não, estão lá por ação da Cyber Crucible. Dependendo da forma como uma aplicação lista os arquivos, poderá vê-los. Por exemplo, um programa que utilize o Explorador de Arquivos para listar arquivos a guardar ou abrir irá agora mostrá-los.

Chamamos a esses arquivos "canaries", como no conceito de “canário na mina de carvão” ([wiki](#)).



O que há de especial nos arquivos-canário da Cyber Crucible?

Os arquivos-canário possuem dados especiais ocultos neles, para o caso de serem roubados por um atacante. A Cyber Crucible consegue rastrear o arquivo até o proprietário original.

Os nomes dos arquivos são majoritariamente aleatórios (chamados de pseudoaleatórios), de forma que os atacantes não conseguem identificá-los e evitá-los. Os nomes são criados com uma fórmula matemática especial da Cyber Crucible, que permite que nosso software reconheça um arquivo como canário, mesmo que os nomes sejam diferentes de máquina para máquina ou de arquivo para arquivo.

A capacidade do software da Cyber Crucible de reconhecer esses arquivos também significa que é necessário apenas um arquivo-canário por servidor, mesmo que milhares de estações de trabalho estejam utilizando o servidor.

Onde existem os arquivos canário?

Os canários são encontrados em vários locais do seu sistema de arquivos.

Sempre que uma nova origem de arquivos aparece no seu sistema, de qualquer usuário possível, o Cyber Crucible verifica automaticamente se já foram colocados canários. Isso inclui unidades removíveis, como pen drives USB, fontes de arquivos de rede e armazenamento de arquivos baseado em nuvem.

Como a Cyber Crucible utiliza a análise de memória?

Os analíticos de kernel da Cyber Crucible acompanham o estado da memória de um programa durante todo o seu ciclo de vida, desde o início até o encerramento do programa. Também monitoram o estado das interações em memória com outros programas.

O monitoramento comportamental verifica estados inseguros na memória do programa. Isso pode significar a ocorrência de uma exploração (exploit), um bug de software ou ataques conhecidos em memória (também chamados de “file-less”).

Esse monitoramento é realizado em tempo real nos programas de maneira altamente eficiente, para garantir que as operações do sistema e do cliente não sejam afetadas pela análise da Cyber Crucible.

No momento em que há possível comportamento de um invasor voltado ao roubo de identidade, roubo de dados ou extorsão, esse rastreamento e análise comportamental de memória é incluído junto com os demais dados de telemetria coletados, a fim de determinar se um programa deve ser suspenso.

Como a Análise Comportamental de Memória da CC difere da varredura de memória?

O Que É a Varredura de Memória?

A varredura de memória é a prática de pegar um bloco de memória, normalmente copiando-o para um local diferente no sistema para análise, e realizar a varredura para análise.

Fotografia vs Ação ao Vivo

Isso não é uma varredura ao vivo do programa enquanto ele se comporta, mas sim uma imagem instantânea do programa em um determinado momento. Pense nisso como uma fotografia, em comparação a uma transmissão ao vivo. O estado do programa pode ser drasticamente diferente de um momento para o outro, portanto, é mais útil como um exercício forense em um ambiente controlado. É menos útil em um ambiente não controlado, como o ambiente de um cliente. Quanto mais ocupada a máquina, ou quanto mais um programa estiver fazendo, mais difícil é obter uma imagem precisa do estado atual de um programa.

A Cyber Crucible começou com um uso intenso de varredura de memória, tentando tirar muitas "fotos" dos estados de memória dos programas. À medida que nos tornamos mais rápidos, encontramos múltiplos gargalos na velocidade com que os snapshots de memória podiam ser feitos, e em múltiplos programas.

Preocupações com o consumo de recursos de CPU ou GPU

Essa varredura de memória pode consumir muitos recursos e pode levar algum tempo para programas grandes. Quando a Cyber Crucible utilizava a varredura de memória, em vez do monitoramento inteligente do comportamento da memória, um núcleo inteiro da CPU era dedicado à varredura.

A Intel possui uma tecnologia inovadora chamada [Intel TDT AMS](#), disponível em arquiteturas específicas baseadas em Intel com uma GPU Intel integrada.

Ela realiza a varredura da memória de um programa quando ele é iniciado pela primeira vez, utilizando a GPU para ajudar a não sobrecarregar a CPU. Além disso, a GPU tem melhor desempenho para o tipo de varredura realizada (mais sobre isso depois).

Metodologia de Varredura

A varredura de memória é realizada para procurar códigos ou "strings" específicos. Estes são frequentemente os mesmos elementos de dados que ferramentas de antivírus/EDR procuram em arquivos potencialmente maliciosos.

A varredura de memória, especificamente, é mais limitada do que algumas das buscas complexas que podem ser realizadas em um arquivo.

Portanto, a varredura, por padrão, procura por itens já conhecidos, como malwares mais antigos, mas é limitada em sua capacidade de fazê-lo.

A Cyber Crucible costumava varrer segmentos de memória em busca de material criptográfico, mas isso se mostrou muito limitado para ambientes modernos, e inventamos um método diferente para observar comportamentos, utilizando lógica baseada em kernel.

Metodologias Baseadas em Comportamento vs Varredura

A Cyber Crucible migrou de uma metodologia baseada em varredura para uma baseada em comportamento por alguns motivos.

Desvantagens da Varredura

A primeira é que uma imagem ao vivo precisava ser utilizada em todos os programas. Os snapshots eram realmente difíceis de completar mesmo para uma análise limitada, antes que

outro fosse necessário. Muita atividade dos programas estava sendo perdida, quase como ter uma câmera de vídeo operando a uma taxa de quadros muito baixa. Isso era agravado pela necessidade de monitorar todos os programas simultaneamente. Servidores ou estações de trabalho ocupadas, sem dúvida os computadores que mais precisavam de monitoramento e que eram mais importantes, acabavam com o menor percentual de vigilância realizada. Independentemente da empresa ou produto, as limitações tecnológicas eram evidentes e inviáveis.

A segunda é que, além do consumo de recursos, a varredura exige, por padrão, procurar por **algo conhecido**. Assim, a varredura de memória precisa ser baseada em assinaturas. Além disso, a varredura por assinatura deve ser um subconjunto limitado da varredura por assinatura mais completa encontrada na varredura de antivírus baseada em arquivos. Os atacantes já vêm evadindo as defesas baseadas em assinaturas de arquivos há anos; há muito pouca chance de os atacantes serem descobertos por um sistema baseado em assinaturas ainda menos capaz.

Vantagens da Análise Comportamental

O monitoramento de memória baseado em comportamento da Cyber Crucible não requer assinaturas e utiliza o acesso à memória do kernel para rastrear os comportamentos de todos os programas simultaneamente. Vamos detalhar isso.

Primeiro, o monitoramento comportamental significa que novos malwares, ou malwares que foram editados por atacantes para parecerem novos, podem ser facilmente descobertos em tempo real. A varredura baseada em assinaturas, seja de memória ou de arquivos, depende de já ter visto aquele malware específico anteriormente. Os atacantes vêm evadindo as defesas baseadas em assinaturas há anos, apesar de um conjunto completo de técnicas de varredura contra arquivos. As técnicas de varredura disponíveis contra a memória são um subconjunto disso, e são ainda menos eficazes.

Segundo, o novo monitoramento comportamental de memória da Cyber Crucible é capaz de permanecer em tempo real em todos os programas simultaneamente, durante toda a execução dos programas. A varredura de memória sofre de graves gargalos de recursos que só pioram à medida que mais programas são executados. Os atacantes normalmente executam dezenas de amostras de malware ao mesmo tempo, sobrecarregando a análise de varredura de memória devido à velocidade e ao número de programas a serem examinados simultaneamente, independentemente de ser um malware de dia zero ou antigo.

O Que Acontece Quando a CC Detecta Ataques de Memória

Primeiramente, é muito importante observar que as alterações de memória ocorrem por vários motivos diferentes:

1. Ataques na memória (in-memory attacks)
2. Interação entre programas
3. Falhas de software (bugs)
4. Exploits

Portanto, uma injeção de processo ou técnica de alteração de memória utilizada, mesmo entre programas, não é necessariamente uma ação maliciosa.

Se um programa que sofreu um evento de memória provavelmente malicioso (ou seja, #1 ou #4 acima) estiver envolvido em uma resposta automatizada por parte da Cyber Crucible, ocorre uma atividade de coleta automatizada.

A parte da memória que foi alterada em um programa, bem como o estado "anterior", é salva em um formato estruturado da Cyber Crucible chamado .ccdif

Essa parte injetada ou alterada da memória é salva e fica disponível para download no portal web da Cyber Crucible.

Por Que Isso Não É Automaticamente Enviado ao Virustotal (etc.) para Análise?

Em algumas circunstâncias, o código malicioso utilizado em um ataque contém variáveis que são exclusivas de um ataque, especificamente relacionadas a uma vítima.

Enviar esse código malicioso a um mecanismo de análise público, como o Virustotal, representaria uma divulgação indesejada de informações que identificam a vítima à comunidade de segurança.

Por Que Seria Útil Enviar Esses Dados Binários ao Virustotal (etc.)?

Ferramentas de antivírus e EDR baseadas em assinaturas procuram por strings ou bytes de código observados em ataques anteriores. Mesmo que esse malware nunca tenha sido visto antes, com o tempo ele pode passar a ser conhecido pela comunidade de segurança. Essas ferramentas de varredura geralmente não precisam que o código esteja em um binário devidamente formatado para sinalizar uma associação com um malware conhecido.

O que é a IA Genética e em que difere de um LLM?

Resposta curta: A IA Genética é a IA de segurança desenvolvida sob medida pela Cyber Crucible. Ela modela como os programas se comportam — na memória, entre processos e em relação a ficheiros — e deteta desvios maliciosos em tempo real. Não é um modelo de linguagem de grande escala (LLM); os LLMs analisam padrões de texto, o que é um problema completamente diferente.

O que a torna diferente

- **Desenvolvida sob medida para a segurança**, e não adaptada a partir de um modelo de texto genérico.
- **Comportamental, não baseada em assinaturas** — sem assinaturas, sem feeds de inteligência de ameaças, sem esperar que outra entidade descubra primeiro o ataque.
- **Totalmente autónoma** — as ferramentas tradicionais dependem da colaboração entre humanos e máquinas; a IA Genética decide e age por conta própria.
- **Pré-execução** — bloqueia o comportamento malicioso antes de este ser executado, em vez de o descrever posteriormente.

IA Vertical

A IA Genética é um exemplo de IA vertical: inteligência artificial personalizada para os desafios específicos de um setor, em vez de um raciocínio de uso geral. Na segurança, essa especialização é o que permite uma decisão sobre a intenção em menos de 200 milissegundos.

Os resultados são mensuráveis — a Cyber Crucible já travou múltiplos ataques de dia zero em redes de clientes até 90 dias antes de qualquer outro fornecedor os ter reportado ou respondido a eles.

Como o Cyber Crucible toma uma decisão em menos de 200 milissegundos?

Resposta curta: Ele executa um ciclo de três etapas — Detect-Decide-Respond — inteiramente no endpoint, ao nível do kernel, utilizando um mecanismo de análise de computação de borda (edge computing) patenteado. Como nada precisa viajar até um serviço na nuvem e voltar, e nenhum ser humano está envolvido no processo, todo o ciclo é concluído em menos de 200 milissegundos.

O ciclo

1. **Detect** — sensores inovadores ao nível do kernel identificam padrões de comportamento malicioso na memória, na atividade de processos e no acesso a arquivos.
2. **Decide** — o modelo comportamental aprimorado por IA avalia instantaneamente a intenção do acesso a dados do programa.
3. **Respond** — se a intenção for maliciosa, o programa é interceptado e suspenso.

Por que o processamento local é inegociável

Enviar telemetria para um servidor na nuvem, aguardar a análise e receber a resposta de volta adiciona milissegundos que o atacante utilizará com prazer. Para se ter uma ideia da escala envolvida: essa decisão ocorre mais rápido do que um impulso nervoso viaja do olho ao cérebro. Qualquer arquitetura que dependa de uma comunicação de ida e volta pela rede no caminho crítico já perdeu essa corrida.

A telemetria bruta ainda é copiada para servidores posteriormente, para fins de evidência e enriquecimento — mas a decisão de proteção nunca espera por isso.

O que é a Rogue Process Prevention (RPP)?

Resposta breve: A Rogue Process Prevention é a abordagem patenteada da Cyber Crucible que consiste em intervir contra um processo malicioso, em vez de apenas observá-lo. Seja um ransomware a iniciar a encriptação, seja um infostealer a tentar obter um token de sessão, o processo é interrompido antes que os dados saiam do dispositivo.

Observar versus intervir

A maior parte do mercado de endpoint está construída para observar. A RPP está construída para intervir. A distinção é a diferença entre uma câmara de segurança que regista um assalto para análise posterior e um guarda que impede o ladrão de chegar ao cofre.

Contra o que protege

A RPP combate os três tipos de ameaças fundamentais em conjunto, porque os ataques modernos são normalmente multifacetados:

- **Roubo de identidade** — acesso a chaves, tokens e palavras-passe, muitas vezes sem qualquer interação por parte do funcionário.
- **Roubo de informação** — exfiltração massiva de dados à velocidade da máquina.
- **Ransomware** — análise comportamental aliada a tecnologia de engano de hackers que impede a encriptação de sequer um único ficheiro.

Uma defesa focada exclusivamente no ransomware deixaria escapar as duas primeiras fases, que são normalmente onde começa o verdadeiro dano.

Que papel a análise de memória desempenha em toda a plataforma?

Resposta curta: A análise de memória é a base sobre a qual tudo o mais é construído. É o sensor e a fonte analítica que alimenta toda a modelagem comportamental — proteção de dados, proteção de identidade e FortressAI igualmente. Cada decisão que essas capacidades tomam depende do conhecimento real do que a memória de um programa está fazendo.

Uma base, três capacidades

A Cyber Crucible rastreia o estado da memória de um programa em todo o seu ciclo de vida, do início ao fim, incluindo suas interações em memória com outros programas. Esse fluxo único de análise é o que torna o restante possível:

- **Proteção de dados** — este processo está se comportando como algo que está prestes a criptografar ou exfiltrar dados?
- **Proteção de identidade** — este processo é o legítimo proprietário da credencial que está tentando acessar, ou foi comprometido?
- **FortressAI** — esta ferramenta de IA ainda é ela mesma, e seu acesso a dados está dentro da política?

Não se trata de três motores separados com três conjuntos de sensores separados. São três políticas expressas sobre o mesmo modelo comportamental de memória.

Por que a memória é a base certa

Os ataques modernos cada vez mais não deixam nenhum arquivo para inspecionar. O código é injetado em processos confiáveis e construído em memória, de modo que o único lugar onde a atividade é visível é o estado de memória de um programa em execução. Uma defesa que não consegue ver ali fica cega para toda essa classe de ataques.

A análise de memória também responde à pergunta mais importante antes de conceder acesso a qualquer coisa sensível: **este programa ainda é o que afirma ser?** Um aplicativo confiável cujo processo ou bibliotecas foram adulterados não é mais confiável, e apenas a inspeção em nível de memória revela isso.

Não é varredura de memória

Isso é rastreamento comportamental em tempo real, não varredura periódica. A varredura copia um bloco de memória e analisa a captura — uma fotografia, em vez de uma filmagem em tempo real. Em uma máquina ocupada, o estado do programa pode ser completamente diferente um instante depois, o que torna as capturas úteis para perícias controladas, mas muito mais fracas para defesa em tempo real.

“ Consulte também os artigos existentes de *Análise de Memória* para detalhes técnicos sobre como isso difere da varredura de memória, e o que ocorre quando um ataque de memória é detectado.

Por que a Cyber Crucible opera no nível do kernel?

Resposta curta: O kernel é a camada mais profunda e privilegiada do sistema operacional. Operar nesse nível permite que a Cyber Crucible veja e controle toda a atividade do sistema, identifique a intenção de um processo malicioso e o interrompa em milissegundos — além de tornar a ferramenta muito mais difícil de ser adulterada ou desativada por um invasor.

O que o acesso ao kernel proporciona

- **Visibilidade completa** sobre o comportamento da memória, o comportamento dos processos e o acesso a arquivos, incluindo atividades que nunca chegam a tocar o disco.
- **A capacidade de agir**, não apenas observar — permissões podem ser revogadas e processos suspensos no momento em que a intenção maliciosa é detectada.
- **Resiliência**, pois os invasores inevitavelmente tentarão desativar a própria ferramenta de segurança.

Sobre as críticas ao desenvolvimento em nível de kernel

Alguns players estabelecidos e analistas desencorajam o desenvolvimento em nível de kernel. A engenharia de kernel é genuinamente difícil e cara, o que explica exatamente por que grande parte do mercado a evitou — e por que os endpoints ficaram dependentes de telemetria em espaço de usuário, que ataques em nível de root conseguem neutralizar.

A qualidade e a resistência à adulteração da Cyber Crucible são validadas pelo Windows Hardware Compatibility Program (WHCP) da Microsoft.

O que significa o facto de a Cyber Crucible ser independente das bibliotecas do Windows?

Resposta breve: A Cyber Crucible não depende das bibliotecas do sistema Windows que está a proteger. Foi deliberadamente dissociada delas, de modo que, quando os atacantes comprometem, bloqueiam ou sequestram essas bibliotecas, a Cyber Crucible continua a funcionar, continua a aplicar as políticas e continua a reportar.

Porque é que isto foi construído

Na segunda metade de 2025, os atacantes passaram a infetar bibliotecas centrais do Windows em memória. Como praticamente todos os fornecedores de segurança dependem dessas mesmas bibliotecas para funcionar, esta única mudança tornou cega uma grande parte do mercado.

A Cyber Crucible passou aproximadamente nove meses a inventar novos sensores e mais cinco meses de esforço de engenharia para eliminar por completo as dependências das bibliotecas do Windows — incluindo a eliminação das dependências voláteis do MiniFilter.

Como isto se apresenta a nível arquitetónico

A arquitetura executa sete subsistemas totalmente independentes dentro do kernel, incluindo a sua própria encriptação isolada, rede, análise de metadados e monitorização de eventos. Uma fase adicional deste trabalho substitui a biblioteca de rede padrão do Windows (`ws32_2.dll`) por uma pilha de rede personalizada ao nível do kernel.

Comprovado em ambiente real

Com dois clientes, os atacantes bloqueados pelo motor de decisão exclusivo do kernel tentaram então impedir que o cliente fosse notificado, atacando a camada de rede do sistema operativo. Como as comunicações de rede da Cyber Crucible são independentes do sistema operativo, a proteção manteve-se e a informação chegou, ainda assim, ao cliente.

A Cyber Crucible funciona offline ou em ambientes isolados (air-gapped)?

Resposta curta: Sim. Toda a análise e a aplicação de políticas ocorrem localmente no endpoint, portanto a Cyber Crucible oferece proteção total sem conexão com a internet, sem serviço em nuvem e sem qualquer tipo de sinal. É adequada para redes isoladas (air-gapped), ambientes OT e ICS, e operações de campo desconectadas.

Por que funciona sem conectividade

Como o ciclo Detect-Decide-Respond é executado inteiramente no kernel do dispositivo, a conectividade nunca é necessária para tomar uma decisão de proteção. A telemetria é sincronizada de forma oportunista para fins de evidência e relatórios quando há conexão disponível, mas a proteção não depende disso.

Comprovado no mar

Em uma implantação marítima, a Cyber Crucible operou de forma independente ao longo de viagens de vários dias sem equipe de TI a bordo, adaptou-se a enlaces de satélite de baixa largura de banda e instáveis, com interrupções causadas por condições meteorológicas, e manteve registros forenses detalhados durante longos períodos desconectados para análise pós-viagem. Os sistemas protegidos variaram desde terminais recreativos voltados aos passageiros até controles marítimos de missão crítica.

É também por isso que o mesmo agente é adequado para chão de fábrica industrial, frotas logísticas e outros ambientes de borda (edge) nos quais a conectividade em nuvem é pouco confiável ou deliberadamente inexistente.

Por que a Cyber Crucible responde suspendendo um processo em vez de desligar o sistema?

Resposta breve: Suspende apenas o processo malicioso — por vezes chamado de Congelamento Seletivo — neutraliza o ataque enquanto tudo o resto continua a funcionar. Não há bloqueio total do sistema, nem reinicialização, nem interrupção do trabalho legítimo.

O problema com respostas do tipo bloqueio total

Quando muitas ferramentas de deteção identificam uma anomalia, as opções de contenção são drásticas: isolar a máquina ou colocá-la offline. Num hospital, numa fábrica ou numa operação de negociação financeira, essa resposta pode ser quase tão prejudicial quanto o próprio ataque.

O que a suspensão seletiva alcança

O ataque é suspenso na memória. As transações legítimas nunca param. Na implementação de serviços financeiros em que quase 10.000 processos maliciosos foram interceptados, as transações SQL legítimas continuaram sem interrupção durante todo o processo — as operações nunca foram interrompidas.

É isso que torna a prevenção compatível com a continuidade dos negócios, em vez de uma escolha de compromisso em relação a ela.