Como a Cyber Crucible se Compara

Respostas diretas às perguntas de comparação e avaliação feitas pelos compradores - versus EDR, XDR, MDR, antivírus, DLP e recuperação baseada em backup.

- A Cyber Crucible é uma EDR, XDR, MDR? Ou algo diferente, como Agentic AI?
- Esta É Uma Ferramenta de Monitoramento Como Meus Outros Painéis de Segurança?
- A Cyber Crucible coexiste com outros produtos de segurança?
- O que acontece se um dos meus produtos de segurança tiver um conflito com o Cyber Crucible?
- Em que é que a Cyber Crucible é diferente de EDR, XDR e MDR?
- A Cyber Crucible substitui o meu EDR, ou funciona em conjunto com ele?
- A Cyber Crucible é um antivírus?
- Por que backup e recuperação não são suficientes para lidar com ransomware?
- Por que capturar chaves de criptografia de ransomware deixou de ser uma defesa válida?
- Por que as ferramentas de segurança baseadas em "coletores em nuvem" enfrentam dificuldades contra ataques modernos?
- A Cyber Crucible torna os meus sistemas mais lentos?

A Cyber Crucible é uma EDR, XDR, MDR? Ou algo diferente, como Agentic AI?

Resposta curta: Ela possui elementos tanto de EDR quanto de XDR, mas a questão da categoria é a pergunta errada. O que importa é *onde a decisão é tomada*. A lógica de resposta da Cyber Crucible é executada inteiramente no endpoint, usando apenas as informações disponíveis ali no momento do ataque — porque servidores analíticos remotos introduzem duas fraquezas fatais: latência e fragilidade.

A resposta honesta à questão do rótulo

- **Como EDR:** se uma EDR usa telemetria de endpoint para tomar decisões, então a resposta automatizada da Cyber Crucible é uma EDR. Ela contém o comportamento de extorsão em milissegundos, usando apenas informações locais.
- **Como XDR:** a telemetria também é enviada a um banco de dados (appliance do cliente ou central) para correlação, caça a ameaças, trabalho contra ameaças internas e auditorias de TI. Pela definição de marketing de XDR, isso se qualifica.

A equipe está confortável com "EDR para defesa contra extorsão", ainda que a computação de borda seja vista por alguns como algo de geração anterior. O raciocínio abaixo explica por que essa visão está equivocada.

Por que a análise remota se tornou uma desvantagem — latência

O "X" em XDR representa a transferência do poder de computação analítica para servidores remotos. Isso traz poder, mas custa tempo, e os atacantes construíram suas táticas em torno dessa lacuna:

- **Velocidade:** os ataques foram acelerados de modo que ações irreversíveis se completem antes que um servidor analítico consiga responder. Isso é especialmente visível com itens pequenos e de alto valor, como senhas.
- **Paralelismo:** muitas ferramentas de endpoint inspecionam um programa por vez, aguardam e então passam ao próximo. Os atacantes executam vários programas de

extorsão simultaneamente — 5.000 arquivos acessados em paralelo em vez de 500.
- **Distribuição:** a extorsão ocorre em muitas máquinas ao mesmo tempo. A Cyber Crucible já observou cerca de 75 máquinas simultaneamente. Uma ferramenta enfrenta então 50 programas em 75 máquinas — 3.750 programas a inspecionar.
- **Processos comandantes:** alguns atacantes executam um controlador local que reinicia instantaneamente qualquer ferramenta de extorsão que seja encerrada.

Estratégias de detecção e resposta, por natureza, esperam que o ataque já esteja em andamento. A analogia mais adequada é impedir assaltantes de banco na porta, em vez de detê-los depois que uma certa quantia já saiu do cofre.

Por que a análise remota se tornou uma desvantagem — fragilidade

Cerca de 80% das soluções de EDR e XDR precisam de acesso a servidores analíticos remotos para funcionar de forma ideal, e ficam praticamente inoperantes sem esse "cérebro" na nuvem.

Os atacantes exploram isso diretamente: obtêm acesso suficiente para alterar regras de firewall, bloqueando a ferramenta de endpoint de alcançar seus servidores analíticos, e a ferramenta perde a capacidade de analisar ou responder. Ela permanece instalada, em execução, não explorada — e praticamente ineficaz.

O que a Cyber Crucible faz em vez disso

Como a latência e a fragilidade tornam a dependência da nuvem insustentável para a defesa contra extorsão, a Cyber Crucible criou uma capacidade de detecção e resposta cuja análise comportamental utiliza **apenas informações disponíveis no endpoint no momento do ataque**. A interdição ocorre localmente, tipicamente em menos de 200 milissegundos, sem nenhuma ida e volta à nuvem no caminho crítico.

A telemetria que é enviada ao banco de dados serve para apoiar investigações, não para proteção — caça a ameaças, detecção de ameaças internas, auditorias de TI — e uma API aberta permite alimentar plataformas XDR abertas, SOAR ou ferramentas de RPA. Esse trabalho é valioso, mas nunca é o que se interpõe entre você e um ataque em andamento.

Esta É Uma Ferramenta de Monitoramento Como Meus Outros Painéis de Segurança?

A resposta é: depende de como você e sua organização desejam utilizar a ferramenta, mas provavelmente "não".

É importante observar as estratégias de design de produto da Cyber Crucible:

1. A proteção deve ser hiperautomatizada, e não deve exigir cuidado e atenção constantes (atenção a alertas), nem ajustes manuais (configuração) por parte dos usuários.
2. Para equipes de segurança com mais recursos, a telemetria valiosa deve estar disponível para elas, para atividades avançadas de caça a ameaças, ou para apoiar atividades de perícia forense e resposta a incidentes.
3. A ação nº 2 acima não deve, de forma alguma, degradar a proteção implementada para a ação nº 1.

O feedback mais comum que recebemos da liderança de TI é que seus funcionários não sabiam que a Cyber Crucible já os estava protegendo há semanas.

Temos muitos usuários que utilizam a ferramenta de três formas:

Configurar e Esquecer (Como Seus Detectores de Fumaça)

Muitas organizações não têm recursos para ter caçadores de ameaças analisando a telemetria da Cyber Crucible (ou de outra ferramenta), mas desejam que o risco de extorsão de dados esteja "fora de sua lista de preocupações". Isso é perfeitamente aceitável, e a Prevenção de Extorsão de Dados da Cyber Crucible foi projetada exatamente para isso.

Esses usuários não têm recursos para dedicar tempo a analisar os feeds de dados de Injeção de Processo, Proteção de Credenciais e Criação de Processo.

Portanto, constatamos que, a menos que estejam respondendo a uma rara resposta automatizada da Cyber Crucible, ou realizando gerenciamento de inventário, como quando uma nova máquina precisa ter a Cyber Crucible implantada nela...

...eles simplesmente não fazem login no portal web da Cyber Crucible, e deixam a automação simplesmente fazer seu trabalho.

Isso é perfeitamente aceitável!

Caça a Ameaças Avançada + Proteção Automatizada

As capacidades de injeção de processo, monitoramento de uso de credenciais e criação de processo fornecem um conjunto rico de dados, capturados por meio de análises comportamentais em nível de kernel, para realizar a caça a ameaças.

A proteção automatizada entra em ação assim que se inicia o roubo de dados, o roubo de credenciais (token, senha) ou a criptografia por ransomware. Para tudo o mais - este é um excelente recurso.

A constatação mais comum até o momento é a presença de ferramentas de gerenciamento remoto não gerenciadas (pelo menos pelos administradores de TI atuais) instaladas pelos usuários. Sim, elas às vezes resultam em uma proteção automatizada contra extorsão (ou seja, a RMM não gerenciada é usada por um agente malicioso), mas é sempre melhor conhecer mais sobre seu ambiente previamente, de qualquer forma!

Aqui está um vídeo rápido de um tipo de ataque que vimos sendo utilizado por atacantes, em múltiplos ambientes de clientes, que foi usado com sucesso para evadir as soluções de EDR dos clientes (preferimos não citar nomes... foram 3 produtos em quatro empresas).

rr-com-dll.mp4

Análise Forense e Remediação Pós-Incidente

Existem alguns tipos de casos de uso para os dados da Cyber Crucible.

O primeiro é para que um profissional de segurança de uma empresa, ou um profissional de TI, possa investigar a causa raiz da suspensão de um programa. Para alguns clientes, que normalmente instalam nosso software e depois só fazem login novamente quando há novos funcionários para integrar, eles nunca usaram nenhuma funcionalidade da Cyber Crucible, exceto a página de Gerenciamento de Agentes. Ficamos felizes em ajudá-los a aprender sobre a análise de

causa raiz - que é indolor e simples para usuários técnicos e semitécnicos.

O segundo tipo de cliente para análise forense pós-incidente são empresas de DFIR que são chamadas para investigar um problema em um cliente, às vezes a pedido da seguradora cibernética, e a Cyber Crucible é instalada após um incidente. (Ei, nem sempre podemos estar lá antes do atacante, por mais que queiramos... caso contrário, todas as empresas do mundo nos teriam, e a extorsão seria coisa do passado!)

A melhor forma de descrever uma implementação após um ataque de extorsão é "confusa". Não porque somos difíceis de instalar ou de começar a proteger. Muito pelo contrário! Nesse caso, os atacantes normalmente já se movimentaram pelo sistema, e estão incorporados em sistemas operacionais, equipamentos de rede, Active Directory, e operam em memória. Várias máquinas acabam tendo processos suspensos, e às vezes os atacantes até tentam recuperar o controle. É um pouco como tomar um remédio que faz você se sentir mal no início, mas que é necessário para melhorar de vez.

Clientes que já estão estressados, às vezes reagem emocionalmente a "mais" ruído, à medida que os atacantes são finalmente descobertos e derrotados. Há muita educação sobre por que ou como suas pilhas de segurança já implementadas não encontraram os atacantes. No final, porém, a empresa recupera o controle sobre sua infraestrutura de TI. Eles não se tornarão uma das 80-90% das empresas que são re-extorquidas um ou dois anos depois, no que chamamos de "economia de assinatura de extorsão".

O terceiro tipo de cliente que temos é um MSSP que, frequentemente, é parceiro da Cyber Crucible, e que está respondendo a uma proteção automatizada da Cyber Crucible. Eles precisam descobrir a forma como o atacante conseguiu obter uma posição temporária, e fechar quaisquer brechas de segurança. A boa notícia é que os relatórios de conformidade com a HIPAA ou outros normalmente reportam pouca ou nenhuma violação de confidencialidade, devido à velocidade da resposta automatizada. Muitas vezes, o MSSP relata "nada a relatar", o que deixa todos os envolvidos satisfeitos. Bem, exceto o criminoso.

A Cyber Crucible coexiste com outros produtos de segurança?

Sim!

A Cyber Crucible está atualmente implantada e coexistindo com todos os fornecedores de segurança do Quadrante Mágico da Gartner.

O nosso software descobre e configura-se automaticamente para ter conhecimento das atividades das outras ferramentas de segurança.

No caso raro de existir um potencial conflito, consulte este artigo da base de conhecimento.

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.

Em que é que a Cyber Crucible é diferente de EDR, XDR e MDR?

Resposta breve: EDR, XDR e MDR são ferramentas de deteção e resposta: observam um ataque, geram um alerta e dependem de um ser humano ou de um serviço na cloud para decidir o que fazer. A Cyber Crucible é uma ferramenta de prevenção: decide de forma autónoma no endpoint e interrompe o processo malicioso em menos de 200 milissegundos, antes de ocorrerem danos.

As diferenças práticas

	EDR / XDR / MDR	Cyber Crucible
Tempo de resposta	Minutos a horas	Menos de 200 milissegundos
Método de deteção	Assinaturas e dados históricos	Intenção comportamental, sem assinaturas
Cobertura de dia zero	Parcial	Concebida para ameaças desconhecidas
Dependência humana	Elevada — analistas e SOCs	Nenhuma — totalmente autónoma
Onde as decisões ocorrem	Análise na cloud	Localmente, no kernel

Porque é que esta diferença importa

As ferramentas de deteção foram concebidas para uma era em que os ataques se desenrolavam ao longo de horas ou dias. Os ataques automatizados concluem-se agora em segundos. Uma ferramenta que produz um alerta preciso depois de os dados terem sido exfiltrados documentou a perda, não a preveniu.

Isto não significa que a deteção não tenha valor — a análise forense e a investigação são importantes. Significa que a deteção por si só não consegue impedir um ataque à velocidade de uma máquina.

A Cyber Crucible substitui o meu EDR, ou funciona em conjunto com ele?

Resposta curta: Ambos. A Cyber Crucible foi concebida para funcionar em conjunto com ferramentas EDR, XDR e MDR existentes, sem conflitos, e muitos clientes implementam-na dessa forma. Também funciona como uma camada de prevenção autónoma, caso decida reduzir o seu conjunto de ferramentas.

Funcionamento em conjunto com o seu conjunto de ferramentas atual

A Cyber Crucible não exige que remova nada. Adiciona prevenção autónoma abaixo da camada de deteção que já possui, e funciona com ou sem EDR e MDR presentes.

Os clientes frequentemente começam desta forma de forma deliberada — implementando a Cyber Crucible para descobrir o que está a faltar no seu conjunto de ferramentas atual. Numa implementação no setor de serviços financeiros, essa resposta chegou em 60 dias: quase 10.000 processos maliciosos foram interceptados, os quais três EDRs e um SOC subcontratado nunca alertaram.

Redução do conjunto de ferramentas

Assim que as equipas percebem com que frequência as suas ferramentas de deteção não atuam, algumas optam por consolidar. Não existe dependência de fornecedor nem integrações forçadas — pode substituir totalmente o seu EDR ou simplesmente cortar despesas onde estas não estão a justificar o seu valor.

A Cyber Crucible é um antivírus?

Resposta curta: Não. O antivírus identifica ficheiros conhecidamente maliciosos utilizando assinaturas. A Cyber Crucible não utiliza assinaturas de forma alguma — avalia o que um programa em execução está efetivamente a fazer e interrompe comportamentos maliciosos, incluindo ameaças nunca antes vistas.

Por que motivo as assinaturas já não são suficientes

Uma assinatura só consegue descrever um ataque que já tenha sido previamente analisado. Este modelo falha em duas situações comuns:

- **Ataques de dia zero (zero-day)**, em que ainda não existe qualquer assinatura.
- **Ataques sem ficheiro (fileless)**, em que não existe nenhum ficheiro contra o qual comparar uma assinatura.

A deteção baseada em assinaturas também exige atualizações constantes provenientes de fontes de inteligência de ameaças, o que significa que a proteção está sempre a reboque do atacante.

O que a substitui

A Cyber Crucible modela o comportamento — atividade de memória, atividade de processos e acesso a ficheiros — e avalia a intenção em tempo real. É por isso que já impediu ataques de dia zero em redes de clientes até 90 dias antes de qualquer outro fornecedor os ter reportado publicamente ou respondido a eles.

Por que backup e recuperação não são suficientes para lidar com ransomware?

Resposta curta: Os backups tratam apenas do estágio final de um ataque de ransomware — a criptografia. Quando a criptografia começa, os atacantes já costumam ter roubado credenciais e exfiltrado seus dados. Restaurar a partir do backup recupera seus arquivos; isso não faz nada em relação aos dados que já estão nas mãos do atacante.

O ransomware é a última etapa, não a primeira

Uma intrusão típica ocorre em três estágios:

1. **Roubo de identidade** — credenciais são comprometidas para obter acesso.
2. **Roubo de dados** — propriedade intelectual, registros de clientes e outros dados sensíveis são exfiltrados.
3. **Criptografia** — arquivos são bloqueados e um resgate é exigido.

As estratégias de recuperação atuam somente no terceiro estágio. A violação de confidencialidade e a perda de controle operacional já ocorreram.

O custo real

O maior risco de negócio decorrente do ransomware geralmente não é o resgate em si — é a receita perdida devido a uma interrupção prolongada e os danos à reputação que se seguem. Prevenir o comprometimento inicial protege ambos, motivo pelo qual a prevenção deve vir antes do planejamento de recuperação, e não em seu lugar.

Por que capturar chaves de criptografia de ransomware deixou de ser uma defesa válida?

Resposta curta: A captura de chaves deixou de ser tecnicamente confiável em 2021. O ransomware moderno evita as bibliotecas de criptografia padrão do sistema operacional, portanto não há chaves para uma ferramenta defensiva interceptar — e mesmo quando as chaves são obtidas, muitas vezes não podem ser aplicadas.

Como o ransomware moderno contorna a captura de chaves

- **Bibliotecas personalizadas:** o código de criptografia é compilado diretamente no malware em vez de chamar bibliotecas do sistema operacional, de modo que as chaves são geradas e usadas inteiramente dentro do processo do próprio invasor — invisíveis para ferramentas que monitoram chamadas padrão.
- **Implementações exclusivas:** algumas variantes usam criptografia não padronizada, específica para cada execução. Mesmo uma chave capturada não pode ser aplicada, porque o próprio algoritmo é personalizado.
- **Cifras de fluxo (streaming ciphers):** construídas sobre um conceito fundamentalmente diferente do AES, são simplesmente imunes à captura de chaves AES.

A Cyber Crucible originalmente desenvolveu e patenteou a tecnologia de captura de chaves e, em seguida, apresentou a criptanálise que demonstrava seus limites na BSides Pittsburgh em 2021. Avançamos porque as evidências assim indicavam.

O problema de conformidade também

A captura de chaves exige o armazenamento centralizado das chaves de criptografia — criando um ponto único de falha e um alvo de alto valor. Um governo também poderia forçar o acesso por meio de uma intimação classificada ou de uma carta de segurança nacional, sem o seu conhecimento. Esse é um risco sério de soberania de dados, somado a uma defesa que já não

funciona.

Por que as ferramentas de segurança baseadas em "coletores em nuvem" enfrentam dificuldades contra ataques modernos?

Resposta curta: Um coletor em nuvem é um agente leve para endpoint que realiza pouca análise local e, em vez disso, envia telemetria bruta para uma plataforma em nuvem para processamento. Essa ida e volta adiciona um atraso que um ataque automatizado não lhe concede, e o agente depende justamente dos componentes do sistema operacional que os invasores atualmente comprometem.

Por que o setor construiu dessa forma

A engenharia em nível de kernel é difícil e cara. Enviar a telemetria para a nuvem permitiu que os fornecedores criassem softwares de endpoint mais baratos, monetizassem o armazenamento em nuvem e divulgassem capacidades de "IA em nuvem". O modelo foi otimizado para facilitar o desenvolvimento, não para a defesa.

Os dois modos de falha

1. **Muito lento.** Ataques automatizados do tipo "smash-and-grab" se completam em milissegundos. As análises em nuvem não conseguem emitir uma resposta a tempo.
2. **Cego justamente quando mais importa.** Como esses agentes dependem de bibliotecas nativas do sistema operacional para funcionar e coletar dados, um invasor que comprometa essas bibliotecas pode silenciar o agente. Ele continua em execução, mas não reporta nada — um painel indicando que está tudo bem enquanto os dados são exfiltrados.

A Cyber Crucible processa localmente no kernel e toma suas próprias decisões, portanto não há ida e volta para a nuvem nem dependência de um sistema operacional potencialmente comprometido.

A Cyber Crucible torna os meus sistemas mais lentos?

Resposta curta: Não. O uso típico de CPU é de cerca de 1% ou menos, e a arquitetura evita deliberadamente a técnica que causa a maioria das lentidões em agentes de endpoint — a inserção de hooks nas bibliotecas de sistema do Windows.

Por que outros agentes causam lentidão

As ferramentas de segurança legadas inserem "hooks" em bibliotecas de sistema altamente otimizadas para observar comportamentos maliciosos. Essas bibliotecas nunca foram projetadas para serem modificadas em tempo real. Quando uma ferramenta de segurança e um atacante estão a manipulá-las ao mesmo tempo, o resultado é uma degradação significativa do sistema.

O padrão que se segue é previsível: o utilizador culpa a ferramenta de segurança pela lentidão e remove-a. O fornecedor não consegue reproduzir o problema em laboratório, sem se aperceber de que um adversário com privilégios de root está a manipular o sistema. Os atacantes aprenderam a explorar isto deliberadamente — degradando o desempenho até as vítimas desativarem as suas próprias defesas.

Uma abordagem diferente

A Cyber Crucible opera através de subsistemas independentes dentro do kernel, em vez de inserir hooks em componentes frágeis do Windows, pelo que não compete com o sistema operativo — nem com um atacante — pelos mesmos caminhos de código frágeis.