Identidade Digital Explicada

O que são realmente tokens de sessão, tokens de atualização, cookies, chaves de API e chaves de carteira, por que os invasores os visam e como o mecanismo comportamental do kernel da Cyber Crucible os protege sem nunca lê-los?

Vocês coletam algum dado de identidade?

A resposta curta é não, não coletamos.

A resposta mais longa é, não, não coletamos, mas de duas maneiras diferentes:

Primeiro, nunca transmitimos senhas, cookies, tokens oauth, ou qualquer outra coisa que seria considerada dado de identidade para nossos servidores da Cyber Crucible. Isso é verdade independentemente de o servidor ser hospedado pelo cliente ou hospedado pela Cyber Crucible.

Segundo, aprendemos a conduzir análise comportamental de informações de identidade, sem de fato processar informações de identidade. Isso significa que nossas análises não estão de fato processando ou expondo dados sensíveis, como senhas reais, tokens de sessão, etc.

Como Isso É Diferente do Monitoramento de Identidade Normal?

A capacidade de proteção contra roubo de identidade digital da Cyber Crucible é proativa e preventiva. Ela impede o acesso às informações necessárias para conduzir operações de chantagem, extorsão e roubo de identidade moderno.

A proteção tradicional contra roubo de identidade lida com senhas e outros dados em posse de fraudadores, e monitora situações como o uso fraudulento de cartões de crédito, a contratação de empréstimos fraudulentos, ou senhas eventualmente encontradas em vazamentos de dados. Isso é muito reativo e é difícil de gerenciar no dia a dia dos clientes. Isso também abre a oportunidade, que a Cyber Crucible já observou, de chantagear indivíduos e até mesmo coagir funcionários e executivos a ajudar os atacantes a atacar seus empregadores.

Há um esforço concentrado por parte dos atacantes para obter cookies, logins, plataformas de mensagens e outras formas de autenticação e dados privados para viabilizar seus ataques.

As análises da Cyber Crucible focadas em roubo de identidade previnem isso, de uma maneira que oferece uma tomada de decisão comportamental autoritativa sem envolvimento do usuário, contra táticas modernas de extorsão e ataques cibercriminosos sem arquivo (fileless).

Quais dados de identidade são protegidos?

Sistema Operacional Windows Principal

- NTDS (Active Directory)
- Recurso em incubação que continuará a melhorar

Credenciais de cliente VPN

- nomes de usuário
- senhas
- autenticação baseada em chave

Navegadores Web

- cookies
- tokens de atualização (tokens de autenticação "lembrar-me")
- tokens oAuth (tokens de sessão, tokens de acesso)
- senhas
- nomes de usuário
- histórico do navegador

Aplicativos de Colaboração e Mensagens

- contatos
- nomes de usuário
- históricos de bate-papo
- conteúdos de bate-papo salvos
- anexos de bate-papo salvos
- chaves de criptografia de mensagens privadas
- senhas
- tokens oauth (tokens de sessão, tokens de acesso, tokens de atualização)

Carteiras de Criptomoedas

- conteúdo das carteiras
- registros de transações
- senhas
- chaves de criptografia

Jogos:

- Em incubação - atualmente apenas Steam
- senhas
- compras
- credenciais
- nomes de usuário
- tokens oAuth (tokens de sessão, tokens de acesso, tokens de atualização)

Compartilhamento de Arquivos:

- Em incubação - atualmente apenas FileZilla
- senhas
- compras
- credenciais
- nomes de usuário
- autenticação baseada em chave
- servidores e configurações de servidor

Como os dados de identidade são protegidos?

Resposta curta: A Cyber Crucible identifica os locais onde os dados de identidade são armazenados e protege esses locais no nível do kernel. Quando um programa tenta acessar um deles, o acesso é rastreado e analisado — **sem que as senhas, tokens ou chaves de criptografia em si sejam acessados ou coletados**. Com base nessa análise, o programa é permitido, recebe dados falsos, é negado ou suspenso.

Protegendo o acesso, não o segredo

A maior parte da proteção de identidade atua sobre o segredo: criptografá-lo, guardá-lo em um cofre ou monitorar seu aparecimento em um vazamento de dados. A Cyber Crucible atua sobre **o ato de tentar acessá-lo**.

Ataques automatizados são previsíveis de uma forma específica — eles precisam ir a locais conhecidos para encontrar credenciais. Os armazenamentos de cookies do navegador, os caminhos de credenciais de VPN, o armazenamento de credenciais do Windows, os arquivos de carteiras (wallets) e os dados do Active Directory estão todos localizados onde os atacantes já sabem procurar. Essa previsibilidade é a oportunidade de defesa.

A Cyber Crucible identifica esses armazenamentos de dados de identidade e, em seguida, os protege. Qualquer programa que toque em um deles é avaliado, junto com seus processos pai e filho e as bibliotecas que carregou.

Os segredos nunca são lidos

Essa é uma restrição de design deliberada, não um efeito colateral: **o acesso é rastreado e analisado sem que a própria credencial seja acessada.** A Cyber Crucible não lê, processa, coleta ou transmite senhas, tokens de sessão, cookies ou chaves de criptografia — para nenhum servidor, seja hospedado pela Cyber Crucible ou pelo cliente.

A análise comportamental do acesso à identidade acaba não exigindo os dados de identidade em si. O que importa é *qual programa está acessando onde, em que contexto, tendo feito o quê anteriormente* — nada disso exige abrir o segredo.

A consequência é que a proteção não pode, ela mesma, tornar-se a violação, e não existe um armazenamento central de suas credenciais para ser intimado judicialmente, vazado ou perdido.

O que o mecanismo comportamental avalia

A decisão não é "este programa está em uma lista?" — é "o que este código está realmente fazendo agora?" Os sinais incluem:

- **Estado e comportamento da memória** — rastreados ao longo de todo o ciclo de vida do programa, incluindo alterações em memória que nunca chegam ao disco. Essa é a camada de sensor fundamental da plataforma, compartilhada com a proteção de dados e o FortressAI, e não é específica da identidade.
- **Linhagem de processos** — o que iniciou isso e o que isso iniciou, por sua vez.
- **Padrão de acesso** — trata-se de uma aplicação normal lendo sua própria credencial, ou de uma varredura simultânea em vários locais de identidade?
- **Atividade de bibliotecas e injeção** — este processo confiável foi injetado ou alterado em memória?

A resposta é graduada, não binária

Nem todo programa que tenta acessar dados de identidade é um atacante, portanto a resposta depende do que o programa é e de como está se comportando:

Situação	Resposta
Uma aplicação conhecida, não explorada, acessando o que legitimamente precisa	Permitido
Uma aplicação conhecida, não explorada, mas que **excede** o acesso apropriado	**Recebe dados falsos, ou o acesso é negado** — regido por regras comportamentais de privacidade
Uma aplicação **desconhecida**	**Rejeitada ou suspensa**, conforme o mecanismo comportamental e suas configurações
Uma aplicação **comprometida** — processo ou bibliotecas explorados	**Rejeitada ou suspensa**, conforme o mecanismo comportamental e suas configurações

O caso intermediário importa mais do que parece à primeira vista. Muitos softwares legítimos acessam os armazenamentos de identidade mais profundamente do que precisam. Suspendê-los prejudicaria o dia do usuário sem qualquer ganho de segurança — mas entregar-lhes credenciais reais é uma exposição desnecessária. Retornar dados falsos satisfaz o programa enquanto o segredo real permanece intacto.

A distinção que o mecanismo está estabelecendo é entre um programa confiável que *excede seu escopo* e um programa que é desconhecido ou que foi *tomado por um atacante*. Somente o último é tratado como um ataque.

Por que isso acontece no endpoint

Um infostealer automatizado pode se infiltrar, coletar e apagar suas próprias ferramentas em memória em questão de segundos. Enviar telemetria para um serviço em nuvem e esperar por um veredito não consegue superar isso. O ciclo completo de detect-decide-respond, portanto, é executado localmente no kernel, o que também é o motivo pelo qual funciona sem qualquer conectividade.

> Veja também: "*Vocês coletam algum dado de identidade?*", "*Quais dados de identidade são protegidos?*" e "*O que acontece quando um programa tenta acessar dados de identidade que não deveria?*"

Quais carteiras de criptomoedas são protegidas?

- Coinomi
- Armory (“Bitcoin Armory”)
- Electrum
- Exodus
- Guarda

O que acontece quando um programa tenta acessar dados de identidade que não deveria?

Resposta curta: Depende de o programa ser confiável e de ter sido comprometido. Uma aplicação legítima que simplesmente se excede recebe dados falsos ou é discretamente negada. Uma aplicação desconhecida ou comprometida é rejeitada ou suspensa. A credencial real nunca é entregue em nenhum desses casos.

Por que uma resposta única estaria errada

O design óbvio é "bloquear tudo o que toca num armazenamento de credenciais". Falha imediatamente na prática, porque o software legítimo toca nesses armazenamentos constantemente — navegadores, gestores de palavras-passe, clientes VPN, ferramentas de sincronização e agentes de cópia de segurança têm todos motivos reais para lá estarem.

Bloquear tudo inutiliza a máquina. Permitir tudo o que é confiável significa que um navegador explorado recebe tudo o que pedir. A pergunta útil é mais específica: **este programa está a comportar-se como deveria?**

Os quatro resultados

1. Permitido. Uma aplicação conhecida e não explorada a aceder ao que legitimamente necessita. Nada muda.

2. Dados falsos devolvidos. Uma aplicação conhecida e não explorada que excede o acesso apropriado. Aplicam-se regras comportamentais de privacidade: o programa recebe dados plausíveis, mas falsos. Continua a funcionar normalmente, e a credencial real nunca sai do armazenamento. Do ponto de vista do programa, nada falhou — e é precisamente por isso que isto funciona sem interromper os fluxos de trabalho.

3. Acesso negado. A mesma situação, em que devolver dados falsos não é apropriado. O pedido é recusado; a aplicação continua a funcionar.

4. Rejeitado ou suspenso. O programa é desconhecido, ou é um programa conhecido cujo processo ou bibliotecas apresentam sinais de exploração. Aqui a preocupação não é o excesso de acesso, é o facto de o programa já não estar a agir como ele próprio. O facto de ser rejeitado ou suspenso depende da avaliação do motor comportamental e das definições que configurou.

Por que enganar em vez de bloquear

Devolver dados falsos é uma escolha deliberada. Um pedido bloqueado diz a um atacante que foi detetado e leva-o a tentar outra via. Dados falsos que parecem reais não fazem isso — a ferramenta prossegue com credenciais que não desbloqueiam nada, e o operador pode não perceber que algo está errado durante algum tempo.

Este é o mesmo princípio por trás dos ficheiros-isco na defesa contra ransomware: dar ao atacante algo convincente para agarrar que não lhe custa nada.

Configurabilidade

O limite entre rejeição e suspensão é ajustável. Ambientes com baixa tolerância a interrupções — sistemas clínicos, linhas de produção — podem privilegiar a negação e os dados falsos em vez da suspensão, enquanto ambientes de alta segurança podem ser mais agressivos.

O que é um token de sessão e por que roubar um é pior do que roubar uma senha?

Resposta curta: Um token de sessão é a credencial que o seu navegador ou aplicação mantém *depois* de você iniciar sessão, comprovando que já está autenticado. Roubar um é frequentemente pior do que roubar uma senha porque isso normalmente contorna tanto a senha quanto a autenticação multifator — o atacante simplesmente retoma a sua sessão existente.

Por que existe

Reintroduzir a senha em cada pedido seria impraticável, por isso, após um início de sessão bem-sucedido, o serviço emite um token. Cada pedido posterior transporta esse token em vez das suas credenciais. O serviço confia nele como prova de que já se autenticou.

Por que os atacantes o preferem

- **Contorna a MFA.** A MFA é verificada no início de sessão. Um token emitido *depois* dessa verificação representa uma autenticação já concluída, pelo que reutilizá-lo normalmente não volta a acionar o segundo fator.
- **Parece legítimo.** Para o serviço, um token válido corresponde a um utilizador válido. Não há sinal de falha de início de sessão nem nada de anómalo para gerar um alerta.
- **É portátil.** Muitos tokens funcionam a partir de uma máquina, rede ou país diferente.

Por que isto mudou o comportamento dos atacantes

Os atacantes evitam cada vez mais permanecer numa rede. Permanecer residente aumenta a probabilidade de deteção. Em vez disso, recolhem material de identidade e saem — regressando depois à vontade como um utilizador autenticado. O token é uma porta dos fundos de aparência legítima que o próprio sistema de autenticação emitiu.

Como a Cyber Crucible resolve isto

O roubo de tokens é interrompido no momento do acesso. Quando um programa tenta aceder ao armazenamento do navegador ou da aplicação onde os tokens residem, o seu acesso é avaliado em menos de 200 milissegundos. Um programa legítimo mas com acesso excessivo recebe dados falsos ou é recusado; um programa desconhecido ou comprometido é rejeitado ou suspenso. Em qualquer dos casos, o token real nunca é entregue.

O que é um token de atualização (refresh token) e por que perdê-lo é especialmente prejudicial?

Resposta breve: Um token de atualização (refresh token) é uma credencial de longa duração usada para obter silenciosamente novos tokens de acesso sem que o usuário precise fazer login novamente. É nisso que a função "lembrar-me" se baseia. Como ele pode gerar acesso renovado indefinidamente, um token de atualização roubado pode conceder a um invasor acesso duradouro muito depois de sua sessão terminar.

Token de acesso vs. token de atualização

- **Token de acesso (token de sessão):** de curta duração, usado a cada solicitação, expira em minutos ou horas.
- **Token de atualização (refresh token):** de longa duração, usado apenas para solicitar novos tokens de acesso. Às vezes válido por semanas ou meses.

Um token de acesso roubado eventualmente expira. Um token de atualização roubado pode ser usado para gerar novos tokens de acesso repetidamente — o que transforma um roubo único em acesso persistente.

Por que "lembrar-me" é uma troca (trade-off)

Permanecer conectado exige armazenar algo duradouro no dispositivo. Essa conveniência é exatamente o que torna o token armazenado valioso para um invasor. Os armazenamentos de credenciais de navegadores e aplicativos são locais padronizados e previsíveis, portanto ferramentas automatizadas vão diretamente até eles.

Reduzindo o dano

Revogar um token de atualização invalida o acesso que ele pode gerar — é por isso que "sair de todos os dispositivos" e a revogação de tokens são importantes após qualquer suspeita de comprometimento. Mas a revogação é uma resposta *após* o roubo.

A abordagem da Cyber Crucible é impedir a leitura. O armazenamento de credenciais é um local protegido: um programa legítimo que ultrapassa seus limites ali recebe dados falsos ou tem o acesso negado, enquanto um programa desconhecido ou comprometido é rejeitado ou suspenso. O token de atualização em si nunca é entregue.

O que são cookies do navegador e como os atacantes os exploram?

Resposta curta: Os cookies são pequenos fragmentos de dados que um site armazena no seu navegador, e alguns deles são cookies de autenticação que mantêm a sua sessão iniciada. Roubar esses cookies é funcionalmente equivalente a roubar uma sessão ativa — o atacante pode carregá-los no seu próprio navegador e passar por si.

Nem todos os cookies têm a mesma importância

- **Cookies de preferências** — idioma, tema, esquema. Valor reduzido.
- **Cookies de análise (analytics)** — medição de utilização. Valor reduzido.
- **Cookies de autenticação / sessão** — comprovam que a sessão está iniciada. **Valor elevado.**

Os atacantes preocupam-se quase exclusivamente com a terceira categoria.

Por que razão o roubo de cookies é eficaz

Um cookie de autenticação roubado normalmente não despoleta um evento de início de sessão, um pedido de palavra-passe, ou um desafio de MFA. A sessão já existe; o atacante está simplesmente a apresentar a prova disso. Do ponto de vista da aplicação, isto parece atividade normal e contínua.

Os navegadores armazenam os cookies em localizações de ficheiros conhecidas e previsíveis em todos os sistemas operativos, pelo que ferramentas automatizadas conseguem localizá-los sem ter qualquer conhecimento sobre a máquina em causa.

Por que razão o navegador é um ponto focal

O navegador reúne num só local os cookies, palavras-passe guardadas, tokens OAuth e o histórico, o que o torna o alvo de identidade mais rico num único ponto na maioria dos terminais. A Cyber Crucible observou isto diretamente: a partir do 4.º trimestre de 2023, as respostas automatizadas contra atividade do Chrome, Edge e Chromium aumentaram de zero para milhares, com CVEs relacionados publicados posteriormente pela Google e pela Microsoft.

Proteção

O armazenamento de credenciais do navegador é uma das localizações de identidade protegidas. Um processo que tente lê-lo é avaliado em contexto — um navegador comprometido é tratado de forma muito diferente de um navegador íntegro, e em nenhum dos casos um pedido excessivo recebe o cookie real.

O que é uma chave de API e o que acontece se ela for roubada?

Resposta curta: Uma chave de API é uma cadeia de caracteres secreta que identifica e autoriza um programa — em vez de uma pessoa — quando este chama um serviço. Uma chave roubada permite que um atacante faça pedidos em nome da sua aplicação, muitas vezes sem qualquer interação do utilizador, sem MFA e sem qualquer sinal evidente de que algo está errado.

Por que são alvos atrativos

- **Sem intervenção humana.** As chaves foram concebidas para uso automatizado e sem supervisão, pelo que não existe qualquer pedido de MFA a interferir.
- **Frequentemente com âmbito demasiado amplo.** As chaves são muitas vezes emitidas com mais permissões do que a tarefa requer.
- **De longa duração.** Muitas nunca são rotacionadas, pelo que uma chave roubada hoje pode continuar a funcionar meses depois.
- **Armazenadas em locais previsíveis.** Ficheiros de configuração, variáveis de ambiente e repositórios de credenciais — todos locais que a automação consegue enumerar.

Consequências típicas

Dependendo do que a chave autoriza: leitura ou exportação de dados de clientes, envio de mensagens em nome da sua organização, gastos financeiros numa conta cloud, ou pivotagem para outros sistemas ligados.

Como os pedidos estão devidamente autenticados, normalmente aparecem nos registos como tráfego normal da aplicação. A deteção ocorre habitualmente muito depois do facto, através de uma fatura ou de uma auditoria.

Redução da exposição

Defina o âmbito das chaves de forma restrita, rotacione-as regularmente e mantenha-as fora do controlo de código-fonte. Estas são boas práticas, mas limitam o raio de impacto em vez de prevenirem o roubo.

A Cyber Crucible visa o próprio roubo. Os locais de credenciais e configuração são protegidos, e um programa que os lê é avaliado em contexto: dados falsos ou recusa em caso de uso excessivo legítimo, rejeição ou suspensão em caso de processo desconhecido ou comprometido. A chave não é entregue em nenhum dos casos.

Onde o Windows armazena senhas e credenciais?

Resposta curta: Em vários locais previsíveis — o Windows Credential Manager, os repositórios de senhas do navegador, a configuração do cliente VPN e, nos controladores de domínio, a base de dados do Active Directory (NTDS). "Previsível" é a palavra-chave: os ataques automatizados dependem do fato de esses locais serem os mesmos em todas as máquinas.

Os principais repositórios

- **Windows Credential Manager** — logins salvos para recursos de rede e aplicativos.
- **Repositórios de senhas do navegador** — Chrome, Edge e Firefox mantêm cada um credenciais salvas em caminhos de perfil conhecidos.
- **Credenciais de cliente VPN** — nomes de usuário, senhas e material de autenticação baseado em chaves.
- **NTDS (Active Directory)** — em um controlador de domínio, os dados de credenciais de todo o domínio. O alvo de maior valor na rede.
- **Repositórios específicos de aplicativos** — ferramentas de mensagens e colaboração, clientes de transferência de arquivos e plataformas de jogos mantêm, cada um, os seus próprios.

Por que a previsibilidade é o cerne da questão

Os atacantes não sabem nada sobre o seu ambiente específico. A automação deles é escrita com base em caminhos que existem em todos os lugares — `C:\Users\[Username]`, pastas padrão de dados de aplicativos, letras de unidade padrão. Um script não precisa entender a sua rede; ele apenas percorre caminhos conhecidos.

Essa é uma fraqueza no método deles. Se esses locais exatos forem os que estão sendo monitorados, o próprio requisito de confiabilidade do atacante se torna o gatilho que o pega.

O que a Cyber Crucible faz com isso

Esses repositórios são os pontos de entrada de roubo de identidade monitorados. A intenção de um programa que os lê é avaliada em menos de 200 milissegundos — e é suspensa se essa intenção for maliciosa, antes que qualquer credencial seja obtida.

O que são chaves de carteira de criptomoeda e por que o roubo é irreversível?

Resposta curta: Uma chave de carteira é a chave criptográfica privada que autoriza gastos a partir de um endereço de criptomoeda. Quem a possui controla os fundos. O roubo é efetivamente irreversível porque as transações em blockchain não podem ser revertidas e não há nenhuma instituição a quem recorrer.

Por que isso difere de um banco

Uma cobrança fraudulenta em cartão pode ser contestada e revertida por um emissor. Uma transação de criptomoeda assinada com sua chave privada é válida por definição — a rede não consegue distinguir um roubo de uma transferência legítima, e não há autoridade central para desfazê-la.

Isso torna as chaves de carteira excepcionalmente atraentes: o retorno é imediato, definitivo e difícil de rastrear.

O que os atacantes procuram

- **Chaves privadas e frases-semente (seed phrases)** armazenadas em arquivos de aplicativos de carteira
- **Conteúdo da carteira e registros de transações** úteis para identificar as vítimas de maior valor
- **Senhas que protegem a carteira**, frequentemente reutilizadas em outros lugares

O software de carteira desktop armazena esse material em locais previsíveis de dados de aplicativos — o mesmo padrão que torna todos os outros repositórios de credenciais acessíveis por automação.

Proteção

Os arquivos de carteira estão entre os locais de identidade que o Cyber Crucible monitora. Como a resposta é a suspensão no momento do acesso malicioso, o roubo é evitado em vez de detectado

posteriormente — o que importa mais aqui do que em quase qualquer outro caso, já que não há caminho de recuperação uma vez que os fundos são movimentados.

> Veja também: "*Quais carteiras de criptomoeda são protegidas?*" para as aplicações específicas atualmente cobertas.

O que é autenticação baseada em chaves e por que chaves roubadas concedem acesso duradouro?

Resposta curta: A autenticação baseada em chaves comprova a identidade com uma chave privada criptográfica em vez de uma senha — utilizada pelo SSH, muitas VPNs e clientes de transferência de arquivos. Uma chave privada roubada concede acesso sem qualquer solicitação de senha ou MFA e, como as chaves raramente são rotacionadas, esse acesso pode persistir por muito tempo.

Como funciona

Você possui uma chave privada; o servidor possui a chave pública correspondente. No momento da conexão, o servidor emite um desafio que somente a chave privada pode responder. A própria chave nunca trafega pela rede.

Isso é genuinamente mais forte do que senhas — resiste a tentativas de adivinhação, phishing e reutilização. Sua fraqueza é diferente: **tudo depende de o arquivo de chave privada permanecer privado.**

Por que uma chave roubada é tão duradoura

- **Nenhuma solicitação de senha.** A chave *é* a credencial.
- **Frequentemente sem MFA.** A autenticação por chave costuma funcionar isoladamente, principalmente em sistemas automatizados.
- **Raramente rotacionada.** Senhas expiram em uma programação; chaves comumente permanecem válidas por anos.
- **Armazenamento previsível.** Diretórios padrão e caminhos de configuração de clientes VPN.

Uma chave roubada é uma porta dos fundos silenciosa e duradoura, que não gera tentativas de login falhas e parece inteiramente legítima.

Proteção

Materiais de VPN e de autenticação baseada em chaves estão explicitamente entre as categorias de identidade protegidas. O acesso é avaliado no nível do kernel, de modo que um programa que colete arquivos de chave é interrompido — negado ou alimentado com dados falsos, caso seja um programa confiável agindo além do esperado, ou rejeitado ou suspenso, caso seja desconhecido ou comprometido — antes que a chave saia da máquina.

Por que a proteção de dados de identidade requer acesso em nível de kernel?

Resposta curta: Porque o roubo acontece no espaço entre um programa que solicita dados de credenciais e o sistema operacional que os entrega. Apenas uma defesa que opera no kernel — abaixo dos aplicativos e bibliotecas que um invasor pode manipular — consegue ver essa solicitação, avaliar sua intenção e impedi-la a tempo.

Os três requisitos

1. Ver o acesso no momento em que ocorre. O roubo de identidade não é um arquivo que aparece no disco; é uma leitura. Ferramentas que buscam arquivos maliciosos não veem nada, porque em um infostealer moderno nada é gravado. O evento a ser detectado é a própria tentativa de acesso.

2. Decidir com rapidez suficiente. Ferramentas automatizadas podem se infiltrar, coletar dados e se autodestruir em segundos. Qualquer arquitetura que envie telemetria para um serviço em nuvem e aguarde um veredito já perdeu a corrida. A decisão precisa acontecer localmente, em milissegundos.

3. Não depender do que o invasor controla. Ferramentas de segurança que dependem de bibliotecas do sistema operacional podem ser cegadas quando um invasor compromete essas bibliotecas em memória — o agente continua em execução, mas não relata nada. O Cyber Crucible foi deliberadamente desacoplado das bibliotecas do Windows, de modo que um sistema operacional comprometido não consegue silenciá-lo.

A consequência

A operação em nível de kernel é o que permite as três coisas simultaneamente: visibilidade sobre a tentativa de acesso, uma decisão local em menos de 200 milissegundos e independência de um sistema operacional potencialmente comprometido.

É também por isso que a proteção funciona sem qualquer conectividade — em ambientes isolados (air-gapped), offline ou no mar — já que nada precisa sair do dispositivo para que uma decisão seja tomada.