

Soluções para o Setor

Como a prevenção autônoma se aplica a setores específicos - saúde, manufatura e OT, serviços financeiros, governo, educação, marítimo e provedores de serviços gerenciados.

- [Como o Cyber Crucible protege ambientes de manufatura, OT e ICS?](#)
- [Como a Cyber Crucible protege empresas de serviços financeiros?](#)
- [Como é que a Cyber Crucible apoia ambientes governamentais e de alta segurança?](#)
- [A Cyber Crucible pode proteger navios e operações remotas ou desconectadas?](#)
- [Por que os MSPs e revendedores fazem parceria com a Cyber Crucible?](#)
- [Fomos vítimas de uma violação recentemente. O Cyber Crucible pode ser implementado num ambiente que já possa estar comprometido?](#)

Como o Cyber Crucible protege ambientes de manufatura, OT e ICS?

Resposta curta: Ele funciona inteiramente no endpoint, sem dependência de nuvem, protegendo assim tecnologia operacional e sistemas de controle industrial que estejam offline, isolados por air gap ou com conectividade intermitente — e suspende apenas o processo malicioso, para que a produção continue em andamento.

Por que as ferramentas convencionais enfrentam dificuldades aqui

Ambientes de OT e ICS não podem tolerar nem uma comunicação de ida e volta com a nuvem, nem um bloqueio total da rede. Muitos são deliberadamente desconectados. Modelos de segurança que pressupõem conectividade constante e um SOC remoto simplesmente não se aplicam.

O que muda

- **100% capaz de operar offline** — proteção completa sem necessidade de sinal, pronta para air gap.
- **Sem bloqueios** — os processos maliciosos são suspensos na memória enquanto a produção continua.
- **Um único agente em todo o ambiente** — o mesmo agente leve protege PLCs no chão de fábrica, veículos em uma rede logística e embarcações no mar, sem a necessidade de um analista humano e sem pressupor conectividade.

Como a Cyber Crucible protege empresas de serviços financeiros?

Resposta rápida: Ela interrompe infostealers e o roubo de tokens de sessão ao nível do kernel, antes que a exfiltração comece, e analisa tudo localmente, de modo que chaves e tokens nunca precisam ser enviados para uma nuvem de terceiros.

A ameaça que as empresas financeiras realmente enfrentam

Ataques hiperautomatizados do tipo "smash and grab" visam tokens de sessão e chaves de API. Eles avançam da infiltração à autoeliminação em segundos — mais rápido do que um alerta na nuvem consegue sair do prédio. Um token de sessão roubado frequentemente contorna senhas e MFA por completo, dando a um atacante uma forma aparentemente legítima de voltar a entrar a qualquer momento.

O caso documentado

Uma grande empresa de serviços financeiros operava três EDRs líderes do setor e um MSSP terceirizado entre os 50 principais. A Cyber Crucible foi implantada para encontrar o ponto cego. Em 60 dias, ela havia interceptado autonomamente quase 10.000 processos maliciosos — 98% deles no farm de servidores Microsoft SQL altamente privilegiados da empresa — sem nenhum alerta da pilha de segurança legada.

A causa raiz foi rastreada a uma credencial de monitoramento remoto provavelmente comprometida. Meses depois, o setor reportou uma onda global de ransomware instalando backdoors em servidores SQL em todo o mundo. O setor financeiro sofreu graves violações. Este cliente nunca foi uma vítima.

Como é que a Cyber Crucible apoia ambientes governamentais e de alta segurança?

Resposta breve: Através de soberania de dados completa — instalação totalmente on-premises em racks fisicamente protegidos, operação em air-gap e arquitetura multi-tenant — sem nuvem pública, sem SOC de terceiros e sem partilha de dados.

Soberania por arquitetura

Para organizações que exigem controlo absoluto, não é necessário que nada saia do ambiente. Não existem plataformas de terceiros no percurso, nem acesso externo, nem análise dos seus dados alojada pelo fornecedor.

Isto é importante porque muitos fornecedores carregam dados de identidade sensíveis — chaves privadas, tokens de sessão — para as suas equipas de SOC alojadas. Esse armazenamento centralizado constitui um ponto único de falha e um alvo de elevado valor para atacantes patrocinados por estados, podendo ainda ser acedido por via de obrigação legal sem o seu conhecimento.

Silencioso por padrão

As ameaças são neutralizadas silenciosamente ao nível do kernel. Só o próprio cliente sabe que um ataque foi tentado e, se nenhum dado tiver sido tocado, normalmente não há alertas externos nem obrigações de divulgação.

Multi-tenant

A arquitetura suporta implementações multi-tenant, o que é adequado para gerir vários departamentos ou agências a partir de uma única instância segura on-premises.

A Cyber Crucible pode proteger navios e operações remotas ou desconectadas?

Resposta curta: Sim, e já o fez. Numa implementação marítima, a Cyber Crucible operou de forma autónoma ao longo de viagens de vários dias sem qualquer equipa de TI a bordo, adaptando-se a ligações de satélite de baixa largura de banda e a longos períodos de desconexão, ao mesmo tempo que protegia tudo, desde terminais de passageiros até controlos marítimos de missão crítica.

O que a implementação demonstrou

- **Resposta autónoma** sem qualquer equipa de TI presente durante vários dias seguidos.
- **Funcionamento adaptado a satélite** em ligações intermitentes, de baixa largura de banda e sujeitas a interrupções meteorológicas.
- **Retenção forense** — registos detalhados preservados durante a desconexão para análise posterior à viagem.
- **Resiliência sob ataque** — manteve-se operacional quando adversários tentaram desativá-la ou degradar o seu desempenho.

A parte invulgar

Os registos revelaram atividade compatível com o envolvimento de um estado-nação, e o alvo foi seletivo: apenas os navios a operar em águas internacionais foram afetados, enquanto os navios de passeio turístico nacionais permaneceram intactos.

Quando as tentativas de intrusão convencionais falharam, os adversários escalaram os ataques — sequestrando credenciais de início de sessão do Windows e, em seguida, alcançando definições ao nível do BIOS para bloquear os sistemas antes do arranque. Mesmo com os sistemas interrompidos antes de o sistema operativo poder carregar, a implementação continuou a manter a linha de defesa onde as pilhas de segurança tradicionais já tinham falhado.

Por que os MSPs e revendedores fazem parceria com a Cyber Crucible?

Resposta curta: Porque a prevenção autônoma permite que um parceiro fique com a margem, o relacionamento com o cliente e o SLA — em vez de revender um SOC hospedado por um fornecedor e assumir a culpa quando esse SOC não detecta um ataque em velocidade de máquina.

A armadilha de revender detecção

O setor empurrou os parceiros para revender serviços de MDR e SOC hospedados por fornecedores. Quando o monitoramento conduzido por humanos inevitavelmente deixa passar um ataque automatizado, o fornecedor perde a violação — e o cliente não demite o fornecedor. Ele demite o parceiro.

O que muda operacionalmente

- As ameaças são neutralizadas instantaneamente, antes que os analistas recebam um alerta.
- O volume de alertas cai drasticamente em relação aos mais de 100 por endpoint por dia que causam a fadiga de alertas.
- Não há ajuste de regras YARA nem caça manual a ameaças.
- Os parceiros capturam o fluxo de receita em vez de se contentarem com comissões do fornecedor.

E do lado do risco

Um parceiro cuja oferta de segurança previne ataques em vez de apenas documentá-los tem uma conversa fundamentalmente diferente com os clientes sobre resultados e responsabilização.

Fomos vítimas de uma violação recentemente. O Cyber Crucible pode ser implementado num ambiente que já possa estar comprometido?

Resposta rápida: Sim. O Cyber Crucible avalia o que os programas estão a fazer neste momento, em vez de procurar ficheiros conhecidos como maliciosos, pelo que começa a impedir comportamentos maliciosos assim que é implementado — incluindo os de um atacante que já tenha conseguido entrar no ambiente.

Porque é que um comprometimento prévio não o "cega"

Como a prevenção se baseia na intenção comportamental ao nível do kernel, um atacante que já esteja presente ainda tem de *agir* — aceder a dados de identidade, injetar-se em processos, iniciar a encriptação ou movimentar dados. São precisamente essas ações que desencadeiam a interceção.

Foi assim que a implementação no setor de serviços financeiros revelou uma intrusão ativa e em curso que a stack de segurança existente nunca tinha sinalizado. O Cyber Crucible não foi implementado para investigar uma violação já conhecida; foi implementado para procurar um ponto cego, e encontrou quase 10.000 processos maliciosos já em curso.

O que esperar

A implementação num ambiente comprometido produz frequentemente uma atividade de interceção imediata e de elevado volume. É a ferramenta a funcionar como previsto, e é muitas vezes a primeira prova concreta que uma organização tem de que algo já estava a acontecer.