Diligência de Fornecedores e Confiança em Segurança

Como a Cyber Crucible responde a questionários de risco de fornecedores de empresas e instituições financeiras — o que a solução armazena e o que não armazena, como apoia obrigações regulatórias, como a IA é governada, níveis de serviço e como sua arquitetura reduz o risco de terceiros. Declarado de forma clara e honesta.

A Cyber Crucible possui um relatório SOC 2?

Resposta breve: Não. A Cyber Crucible não possui atualmente uma certificação SOC 2, e afirma isso claramente em vez de sugerir o contrário. O motivo é arquitetural: a Cyber Crucible é um produto de software de execução local, não um custodiante em nuvem de dados de clientes, portanto o modelo de organização de serviços do SOC 2 — que atesta como um fornecedor armazena, processa e transmite *seus* dados em seus próprios sistemas — não se aplica diretamente a ela.

Por que a maioria dos clientes não exigiu um

O SOC 2 atesta os controles de uma organização de serviços que detém dados de clientes. O design da Cyber Crucible elimina essa premissa:

- A detecção e resposta a ameaças ocorrem no endpoint, em nível de kernel, no próprio dispositivo do cliente.
- Arquivos, credenciais, chaves de criptografia e tokens de sessão do cliente nunca são coletados, transmitidos ou armazenados pela Cyber Crucible.
- A plataforma pode ser totalmente implantada on-premises ou em ambiente isolado (air-gapped), dentro da própria infraestrutura do cliente.

Como as categorias de dados de maior risco nunca estão sob a custódia da Cyber Crucible, grande parte da superfície de risco de fornecedor que o SOC 2 se destina a abordar é eliminada por design, e não meramente controlada.

O que existe em seu lugar

Para avaliadores que trabalham a partir de um questionário, a Cyber Crucible fornece um pacote de segurança de fornecedor previamente preparado, que apresenta diretamente as evidências de controle subjacentes e mapeia seus controles aos Critérios de Serviços de Confiança (Trust-Service Criteria) do SOC 2 e ao NIST Cybersecurity Framework, permitindo que um avaliador complete um questionário padrão com base nele. O pacote está disponível mediante acordo mútuo de confidencialidade (NDA) através do e-mail **dpo@cybercrucible.com**.

O plano de conformidade e garantias é mantido em avaliação contínua conforme as necessidades dos clientes; esta página será atualizada caso essa posição mude.

A Cyber Crucible é certificada em ISO 27001, PCI-DSS, CMMC ou FedRAMP?

Resposta curta: Não. A Cyber Crucible não obteve, nem reivindica, certificação ou autorização ISO/IEC 27001, PCI-DSS, HIPAA, CMMC ou FedRAMP. Isto é afirmado diretamente, porque reivindicar uma certificação que um fornecedor não possui é exatamente o tipo de inconsistência que compromete a confiança numa análise de due diligence.

O que isto significa na prática

- **PCI-DSS:** a Cyber Crucible não processa, armazena nem transmite dados de titulares de cartão, pelo que está fora do âmbito enquanto processadora de dados de cartão, ao mesmo tempo que continua a apoiar os objetivos de controlo de segurança de endpoint de um cliente.
- **HIPAA:** uma vez que não é recolhido conteúdo do cliente, a Cyber Crucible evita criar uma relação de custódia de informação de saúde protegida; pode ser celebrado um Acordo de Associado Comercial (Business Associate Agreement) quando um cliente o exigir.
- **ISO 27001 / CMMC / FedRAMP:** não são detidas, nem representadas como sendo detidas.

O que a Cyber Crucible efetivamente possui

Existe validação independente e objetiva onde mais importa — consulte *Que validação de segurança independente possui a Cyber Crucible?* As referências a frameworks presentes noutras partes desta base de conhecimento são mapeamentos de autoavaliação que ajudam um revisor a relacionar os controlos da Cyber Crucible com uma norma que já utiliza; não são pareceres de auditoria de terceiros.

Que validação de segurança independente a Cyber Crucible possui?

Resposta curta: Os drivers de kernel do Windows da Cyber Crucible são objetivamente testados e assinados criptograficamente sob o Windows Hardware Compatibility Program (WHCP) da Microsoft. Trata-se de uma atestação externa e independente da qualidade e da resistência a adulterações do componente mais privilegiado do produto — o código onde a correção é mais crítica.

Por que o WHCP é significativo

A maior parte do mercado de endpoint evitou o desenvolvimento em nível de kernel porque isso é genuinamente difícil e caro. A Cyber Crucible opera no kernel de forma deliberada e submete seus drivers ao programa da Microsoft para que uma parte externa — não apenas a Cyber Crucible — valide que o código mais sensível está correto e é resistente a adulterações.

- A validação é **delimitada precisamente ao driver**, não sendo apresentada como uma certificação de todo o produto.
- Trata-se de um teste objetivo e repetível, e não de uma auditoria administrativa subjetiva.

Como isso se encaixa no panorama geral

Para um avaliador acostumado a procurar um relatório SOC 2, o WHCP é um dado concreto e independente que um SOC 2 não fornece: a validação direta do componente de kernel. Ele complementa — em vez de substituir — as evidências de controle presentes no pacote de fornecedor preparado pela Cyber Crucible.

Como a Cyber Crucible apoia a GLBA e os requisitos para fornecedores de instituições financeiras?

Resposta breve: Como fornecedora de serviços de software para uma instituição financeira, a Cyber Crucible apoia as obrigações da instituição no âmbito das expectativas de proteção (Safeguards) da GLBA e das diretrizes interagências de segurança da informação — principalmente por nunca coletar as informações pessoais não públicas (NPI) que essas normas foram redigidas para proteger. A Cyber Crucible é uma fornecedora de software, não uma instituição financeira licenciada, portanto não é ela própria examinada; seus controles são projetados para serem examináveis como parte do programa de gestão de risco de terceiros da instituição.

Onde a arquitetura faz o trabalho

- **Nenhuma NPI coletada.** O produto é executado em endpoints que podem lidar com NPI sem extraí-las. Não há informações financeiras de consumidores para a Cyber Crucible usar, compartilhar ou redivulgar, o que apoia diretamente a posição da Regra de Privacidade da GLBA / Regulamento P.
- **Programa de segurança documentado.** Controle de acesso, criptografia, resposta a violações e controle de mudanças são documentados e passíveis de evidência — as proteções que o programa de um banco procura em um fornecedor de serviços.
- **Evidências de due diligence disponíveis.** Um pacote de fornecedor previamente preparado é estruturado para servir como evidência de due diligence e monitoramento contínuo que um banco precisa segundo as diretrizes interagências atuais de risco de terceiros.

O limite honesto

A Cyber Crucible apoia as obrigações de conformidade de um cliente; ela não torna, por si só, uma organização compliant, e isto não constitui aconselhamento jurídico. Detalhes específicos, com qualidade de evidência, são fornecidos aos revisores de um banco mediante NDA. Veja também *A Cyber Crucible atende às expectativas da FFIEC e de gestão de risco de terceiros?*

A Cyber Crucible atende às expectativas da FFIEC e de gestão de risco de terceiros?

Resposta curta: A Cyber Crucible foi concebida para ser examinável em relação às expectativas de segurança, operações e continuidade de negócio que os examinadores aplicam à tecnologia bancária, e o seu pacote preparado para fornecedores está organizado para servir como evidência de due diligence de que uma instituição financeira necessita ao abrigo da orientação interagências de 2023 sobre relações com terceiros.

No que o programa de um banco se pode basear

- Detalhe de controlos mapeado para os domínios encontrados em questionários padrão (SIG, CAIQ) e para os Trust-Service Criteria do SOC 2 e o NIST CSF.
- Validação independente de drivers (WHCP) como atestação externa de qualidade.
- Uma postura de continuidade de negócio documentada e testada, com a propriedade importante de que a proteção de endpoint continua mesmo durante uma indisponibilidade do backend de gestão.
- Evidência de seguros, informação financeira e uma lista de subprocessadores disponibilizadas aos revisores mediante pedido.

Por que a arquitetura reduz o risco de terceiros

O facto mais útil para um analista de risco de fornecedores de um banco é que a Cyber Crucible nunca recolhe ficheiros, credenciais ou chaves de clientes. Os dados que preocupam um revisor quanto a um manuseamento indevido por parte de um fornecedor não estão sob a custódia da Cyber Crucible para serem mal geridos. Trata-se de uma redução estrutural do risco, não de uma promessa de o gerir bem.

A que estruturas de segurança e conformidade a Cyber Crucible se alinha?

Resposta curta: A Cyber Crucible mapeia os seus controlos para o NIST Cybersecurity Framework, as famílias de controlos NIST SP 800-53 relevantes e os CIS Critical Security Controls, e mapeia também para os Critérios de Serviços de Confiança (Trust-Service Criteria) do SOC 2 para conveniência do avaliador. Estes são **alinhamentos autoavaliados**, disponibilizados para que um avaliador possa relacionar os controlos da Cyber Crucible com uma norma que já conheça — não são certificações nem pareceres de auditoria de terceiros.

Alinhamento, declarado com honestidade

Estrutura	Estado
NIST Cybersecurity Framework (CSF)	Controlos autoavaliados; não é uma certificação
Famílias de controlos NIST SP 800-53	Alinhado onde aplicável; não é uma autorização
CIS Critical Security Controls	Alinhado; não certificado
Critérios de Serviços de Confiança do SOC 2	Mapeado para conveniência do avaliador; nenhum relatório detido
Microsoft WHCP (controlador)	Detido — uma validação externa e independente

Por que dizer isto desta forma

Um fornecedor que lista estruturas para as quais não foi auditado convida o avaliador a desconfiar de todas as outras respostas. A Cyber Crucible declara o que é uma certificação (WHCP) e o que é um mapeamento autoavaliado (o restante), para que um avaliador possa ponderar cada um em conformidade.

A Cyber Crucible utiliza IA e é um modelo de linguagem de grande porte?

Resposta curta: A Cyber Crucible utiliza IA proprietária — mas apenas durante o desenvolvimento, não no seu endpoint, e não se trata de um modelo de linguagem de grande porte. Sua Genetic AI é uma ferramenta de descoberta em tempo de design que identifica o conjunto determinístico de variáveis comportamentais que indicam um ataque. Essas descobertas se tornam heurísticas fixas e determinísticas em nível de kernel. Em tempo de execução, nenhuma IA, nenhum LLM e nenhum modelo adaptativo é executado no dispositivo.

Por que isso representa uma posição mais forte, não mais fraca

- **Nenhum modelo em tempo de execução significa nenhum desvio (drift).** O comportamento do endpoint é determinístico, repetível e testável — não probabilístico.
- **Nenhuma superfície de inferência ativa.** Não há modelo no dispositivo que um invasor possa manipular ou envenenar.
- **Nenhum dado de cliente em qualquer modelo.** Conteúdo, credenciais e chaves do cliente nunca são usados para treinar, alimentar ou ajustar um modelo, e nenhum dado do cliente sai do endpoint para processamento de IA.

Para um avaliador de instituição financeira ou de setor regulado, essa costuma ser a resposta sobre IA que esperam ouvir: capacidade sem um modelo ativo e opaco tomando decisões no endpoint.

Relacionado

Veja *Como a IA é governada no ciclo de vida de desenvolvimento da Cyber Crucible?* para saber como o trabalho em tempo de design é controlado.

Como a IA é governada no ciclo de vida de desenvolvimento da Cyber Crucible?

Resposta rápida: Como a Genetic AI da Cyber Crucible é usada apenas em tempo de design, ela é governada sob o ciclo de vida de desenvolvimento seguro (SDLC) e não como um sistema de produção ativo. O trabalho de descoberta ocorre em um ambiente interno controlado, seu resultado é validado e traduzido em heurísticas determinísticas do kernel, e os drivers resultantes são assinados de forma independente sob o Microsoft WHCP antes do lançamento.

O ciclo de vida governado

Fase	Governança
Design	Requisitos de segurança definidos; a descoberta por IA faz parte da fase de design, sob o SDLC
Descoberta	A Genetic AI identifica variáveis determinísticas indicadoras de ataque usando apenas conjuntos de dados de pesquisa internos
Derivação	As descobertas se tornam heurísticas de kernel fixas e determinísticas — nenhum modelo ativo é implantado
Validação	Os resultados determinísticos são repetíveis e testáveis; modelos e drivers validados por meio de QA
Lançamento	Drivers do Windows assinados pelo WHCP; alterações seguem a gestão formal de mudanças

Dados e integridade

Nenhum conteúdo, credencial ou chave de cliente é usado para treinar, alimentar ou ajustar um modelo. Os modelos são proprietários e desenvolvidos internamente, sem dependência de modelos de terceiros. A integridade do modelo é mantida por meio de controle de versão, validação SDLC/QA e assinatura WHCP; a confidencialidade, por meio de um ambiente de desenvolvimento controlado.

Onde são processados os dados da Cyber Crucible — são armazenados na nuvem?

Resposta breve: A análise de ameaças e a resposta ocorrem localmente no endpoint, não na nuvem. A Cyber Crucible não coleta arquivos, credenciais ou chaves dos clientes, e não armazena conteúdo dos clientes com um provedor de nuvem pública terceirizado. O backend de gestão e relatórios é executado em infraestrutura operada pela Cyber Crucible, localizada nos Estados Unidos, e uma implantação totalmente on-premises ou isolada (air-gapped) está disponível para organizações que exigem fluxo zero de dados externos.

Por que o processamento local é importante

- **A decisão de proteção nunca sai do dispositivo.** O Detect-Decide-Respond é executado no kernel, no próprio endpoint, tipicamente em menos de 200 milissegundos, sem ida e volta à nuvem no caminho crítico.
- **Proteção independente do backend.** Uma interrupção no backend de gestão não reduz a proteção do endpoint.
- **Escolha de implantação.** Organizações com mandatos rigorosos de residência ou soberania de dados podem executar a Cyber Crucible inteiramente dentro de sua própria infraestrutura segura.

No que um revisor pode confiar

Como o conteúdo dos clientes nunca é coletado, a pergunta "para onde vão os nossos dados?" tem uma resposta simples para as categorias de maior risco: eles não vão para lugar nenhum. Informações detalhadas sobre infraestrutura e subprocessadores são fornecidas aos revisores mediante acordo de confidencialidade (NDA).

Qual é a disponibilidade de serviço e o SLA de suporte da Cyber Crucible?

Resposta curta: O Contrato de Nível de Serviço (SLA) publicado pela Cyber Crucible estabelece um compromisso de **99,9% de disponibilidade mensal do serviço** (excluindo manutenção programada e causas fora do seu controlo razoável), com um mecanismo de compensação por tempo de inatividade previamente definido. Os tempos de resposta do suporte são escalonados por gravidade, medidos a partir da abertura do ticket através do portal de suporte.

Metas de tempo de resposta do suporte

Gravidade	Descrição	Resposta
SEV1 — Crítica	Serviço em baixo ou com impacto crítico na produção; sem solução alternativa disponível	≤ 2 horas
SEV2 — Grave	Serviço afetado de forma a limitar a proteção ou a resposta	≤ 4 horas
SEV3 — Menor	Serviço afetado sem impacto na proteção ou na resposta	≤ 12 horas
SEV4 — Menor	Problema não crítico, pedido de informação ou sugestão de melhoria	≤ 48 horas

Onde encontrar

O Contrato de Nível de Serviço completo está disponível publicamente em cybercrucible.com/service-level-agreement, e os tickets de suporte são registados em support.cybercrucible.com. Um prazo comprometido para notificação de violação ou incidente pode ser estabelecido contratualmente para clientes sujeitos a regulamentação.

Uma nota sobre a disponibilidade

Uma vez que a proteção de endpoint é executada localmente, o valor de disponibilidade aplica-se ao backend de gestão e de relatórios. A proteção no próprio dispositivo continua a funcionar mesmo que o backend esteja temporariamente indisponível.

Como a Cyber Crucible lida com a retenção e exclusão de dados?

Resposta curta: A Cyber Crucible minimiza o que armazena e retém dados apenas pelo tempo necessário para fornecer o serviço. Ela nunca coleta conteúdo, credenciais ou chaves do cliente, portanto as categorias de maior risco não têm nada a reter. A telemetria comportamental e os metadados de segurança derivados são descartados de acordo com cronogramas definidos e, ao final de um contrato, todos os dados associados são disponibilizados para exclusão, com confirmação.

O princípio

- **Minimizar primeiro.** Os dados mais sensíveis nunca são coletados, portanto não há nada nessas categorias para reter ou destruir.
- **Reter por finalidade.** A telemetria comportamental e os metadados de segurança são mantidos apenas enquanto servirem à detecção, investigação e geração de relatórios, sendo descartados em seguida.
- **Excluir na saída.** Ao final do contrato, os dados associados são disponibilizados para exclusão e a Cyber Crucible fornece confirmação.

O que é documentado

Um processo documentado de destruição abrange tanto informações impressas quanto eletrônicas. Os períodos específicos de retenção por tipo de dado são fornecidos aos avaliadores sob acordo de confidencialidade (NDA) e podem ser reduzidos por contrato.

A Cyber Crucible tem um Responsável pela Proteção de Dados?

Resposta curta: Sim. A Cyber Crucible contratou um Responsável pela Proteção de Dados (DPO), com experiência multijurisdicional abrangendo o RGPD da UE/Reino Unido, a CCPA/CPRA da Califórnia, a HIPAA, o PCI-DSS e regimes globais de proteção de dados, incluindo a PDPL da Arábia Saudita. O DPO pode ser contactado através da caixa de correio monitorizada **dpo@cybercrucible.com**.

O que o DPO abrange

- O programa de privacidade e os acordos de processamento de dados.
- Avaliações de impacto sobre a proteção de dados e de risco de transferência, incluindo as Cláusulas Contratuais-Tipo para transferências transfronteiriças.
- Determinações relativas à notificação de violações e apoio às próprias obrigações de notificação do cliente.
- Um ponto de contacto qualificado para questões de privacidade e conformidade durante o processo de aquisição.

Porquê um DPO contratado com experiência global

Vários regimes fora dos EUA — entre os quais a PDPL saudita — podem ser mais restritivos do que a legislação atual dos EUA. Contratar um DPO com domínio do RGPD, da CCPA/CPRA, da HIPAA e das PDPLs globais permite à Cyber Crucible apoiar os clientes de acordo com o padrão mais rigoroso, o que geralmente satisfaz o nível base dos EUA como um subconjunto.

A Cyber Crucible está sujeita aos controles de exportação dos EUA?

Resposta breve: Sim — o software da Cyber Crucible está sujeito ao Export Administration Regulations (EAR) do Departamento de Comércio dos EUA. Ele **não** é controlado pelo ITAR e não é administrado pelo Departamento de Estado. Não é necessária nenhuma licença especial para fornecer o software aos clientes, e a classificação e triagem de exportação são tratadas como parte do programa de conformidade da Cyber Crucible.

O que isso significa para um comprador

- **EAR, não ITAR.** O produto está sob a jurisdição do Departamento de Comércio, a estrutura que se aplica à maioria dos softwares comerciais com recursos de criptografia — não ao regime de artigos de defesa.
- **Patenteado e revisado.** A tecnologia foi patenteada internacionalmente após revisão do Escritório de Patentes e Marcas Registradas dos EUA (USPTO), que incluiu revisão do Departamento de Defesa.
- **Sem barreira de licenciamento.** Fornecer o software a um cliente não requer uma licença de exportação especial.

Detalhes sobre a classificação de exportação estão disponíveis para avaliadores mediante solicitação.

Como é que a Cyber Crucible reduz o risco de terceiros e fornecedores para compradores regulados?

Resposta breve: Eliminando o risco em vez de apenas o gerir. Os três factos que respondem às perguntas mais difíceis sobre risco de fornecedores são: a Cyber Crucible não recolhe conteúdo, credenciais ou chaves de clientes; a proteção funciona localmente e sobrevive a qualquer falha do backend; e a sua IA existe apenas em fase de desenvolvimento, nunca no seu endpoint. Em conjunto, estes factos reduzem a superfície que uma revisão de due diligence é concebida para investigar.

Os três fatores estruturais de redução de risco

- **Zero conteúdo.** Nenhum ficheiro, credencial ou chave de cliente é alguma vez recolhido. Este único facto responde às linhas de questionamento relativas a PCI, dados confidenciais e "e se forem alvo de uma violação" — os dados simplesmente não existem para serem perdidos.
- **Proteção independente do backend.** O Detect-Decide-Respond funciona localmente, com um objetivo de tempo de recuperação (RTO) efetivo de zero no endpoint. Uma falha total do backend não reduz a proteção.
- **IA determinística.** A IA é utilizada apenas em fase de desenvolvimento; heurísticas determinísticas são executadas em tempo de execução. Sem modelo em funcionamento contínuo, sem desvio (drift), com resultados testáveis.

Reforço independente

Sempre que a certificação independente tem peso, a Cyber Crucible remete para o que é real: a assinatura de drivers Microsoft WHCP e — no caso do backend gerido — as certificações de terceiros dos fornecedores de infraestrutura de que depende. Sem uma certificação SOC 2 própria, estes elementos sustentam a argumentação de forma honesta, sem exageros.

Como posso obter o pacote de due diligence de segurança da Cyber Crucible?

Resposta rápida: Solicite-o através de **dpo@cybercrucible.com**. Ao abrigo de um NDA mútuo, a Cyber Crucible disponibiliza um pacote de segurança para fornecedores previamente preparado, que responde aos domínios dos questionários padrão (SIG, CAIQ) e substitui um relatório SOC 2 nos casos em que um revisor normalmente procuraria um.

O que o pacote e os seus documentos complementares incluem

- Um pacote de segurança e confiança para fornecedores previamente preparado: arquitetura, tratamento de dados, encriptação, gestão de acessos, desenvolvimento seguro, resposta a incidentes, continuidade de negócio, alinhamento regulatório e um mapeamento de estrutura de controlos.
- Resumos de programa de uma página para conformidade, auditoria e governação de IA/SDLC.
- Um certificado de seguro, W-9 e informação financeira, disponíveis mediante pedido.
- Cláusulas Contratuais Padrão, uma Avaliação de Risco de Transferência e um Acordo de Processamento de Dados, disponíveis mediante pedido.

Documentos públicos que pode consultar já

Documento	Localização
Acordo de Nível de Serviço	cybercrucible.com/service-level-agreement
NDA Mútuo	cybercrucible.com/mutualNDA
MSA e EULA	cybercrucible.com/msa-and-eula
Política de Privacidade	cybercrucible.com/privacy-policy

Tudo o que exceda os acordos públicos é fornecido aos revisores ao abrigo de NDA, sujeito a medidas de confidencialidade razoáveis.