Guias de Risco de Fornecedores do Setor

Respostas de due diligence de segurança para setores regulados específicos — saúde, educação, governo, defesa, serviços públicos, serviços financeiros, varejo, jurídico e seguros — estruturadas para o revisor de risco de fornecedores. Declara claramente o que a Cyber Crucible possui e não possui.

Como a Cyber Crucible apoia a conformidade com a HIPAA, e a empresa assinará um Acordo de Associado Comercial (Business Associate Agreement)?

Resposta breve: A Cyber Crucible apoia as obrigações de uma entidade coberta (covered entity) pela HIPAA principalmente por nunca coletar informações de saúde protegidas (PHI). A análise ocorre localmente no endpoint, portanto a PHI não é enviada para uma nuvem de terceiros para processamento de segurança. Como a Cyber Crucible não cria, recebe, mantém ou transmite PHI em nome de uma entidade coberta, ela normalmente não se enquadra na definição de associado comercial (business associate) — mas, quando o processo de risco de um cliente exigir, um Acordo de Associado Comercial pode ser firmado.

Por que a arquitetura é adequada para a área da saúde

- **A PHI nunca sai do dispositivo para análise de segurança.** Muitos acordos de SOC/MDR hospedados por fornecedores enviam arquivos, chaves ou telemetria para uma nuvem de terceiros; a Cyber Crucible realiza a análise no endpoint, evitando essa exposição.
- **Continuidade clínica.** Apenas o processo malicioso é suspenso — sem isolamento total do sistema ou reinicialização forçada — de modo que os dispositivos conectados e os sistemas clínicos continuam em funcionamento enquanto um ataque é neutralizado.
- **Ransomware sem a necessidade de um SOC 24/7.** A prevenção autônoma interrompe os ataques antes da execução, sem exigir analistas que um hospital talvez não consiga manter em sua equipe.

O limite honesto

A Cyber Crucible não é "certificada pela HIPAA" — não existe tal certificação. Ela apoia o seu programa de conformidade; seus responsáveis pela privacidade e segurança fazem a determinação adequada para o seu ambiente. Um BAA está disponível mediante solicitação em **dpo@cybercrucible.com**.

Como é que a Cyber Crucible apoia a FERPA e a privacidade de dados de estudantes em escolas e universidades?

Resposta breve: A Cyber Crucible ajuda instituições de ensino de duas formas: interrompe o ransomware de forma autónoma sem necessidade de um centro de operações de segurança (SOC) 24/7, e — através da FortressAI — avalia o acesso a dados por ferramentas de IA no dispositivo, para que os registos dos estudantes e os dados familiares não cheguem acidentalmente a um sistema de IA público. Como a análise é local e não são recolhidos registos de estudantes, os registos educativos protegidos permanecem dentro do perímetro da instituição.

Os dois problemas educativos abordados

- **Ransomware sem um SOC.** A prevenção ao nível do kernel interrompe os ataques em menos de 200 milissegundos, sem necessidade de contratar analistas nem de financiar um contrato de monitorização contínua 24/7.
- **Governação de IA para a sala de aula.** A FortressAI verifica cada instrução (prompt) no dispositivo, para que os registos educativos protegidos e os dados pessoais familiares não sejam enviados para um sistema de IA público — incluindo como dados de treino.

Notas para a seleção de fornecedores

- A Cyber Crucible atua como funcionário escolar / prestador de serviços sob a direção da instituição e não utiliza os dados dos estudantes para qualquer finalidade secundária.
- As leis estaduais de privacidade de estudantes (por exemplo, na Califórnia, em Nova Iorque e no Colorado) acrescentam obrigações adicionais aos fornecedores; o design de processamento local e sem recolha de dados dá suporte a essas exigências. A documentação está disponível mediante acordo de confidencialidade (NDA).

A Cyber Crucible possui autorização FedRAMP e como atende agências governamentais?

Resposta curta: Não — a Cyber Crucible não possui atualmente uma autorização FedRAMP, nem sugere o contrário. O FedRAMP autoriza ofertas de serviços em nuvem que armazenam dados de agências; o modelo da Cyber Crucible é diferente. Ele é executado localmente no endpoint e pode ser implementado totalmente on-premises ou em ambiente isolado (air-gapped) dentro do próprio perímetro da agência, de modo que os dados da agência nunca saem desse perímetro em direção a uma nuvem de terceiros.

Como a arquitetura se adequa ao setor público

- **Implementação on-premises / air-gapped.** A plataforma pode ser executada inteiramente dentro da infraestrutura segura de uma agência, sem qualquer fluxo externo de dados — adequada para ambientes classificados, desconectados e de alta segurança.
- **Nenhum dado da agência é coletado.** Conteúdo do cliente, credenciais e chaves nunca são coletados, o que elimina grande parte daquilo que uma autorização em nuvem se destina a proteger.
- **Fabricado nos EUA e sujeito a controle de exportação.** O software está sujeito ao EAR do Departamento de Comércio dos EUA (não ao ITAR), e é patenteado internacionalmente após revisão do USPTO que incluiu análise do Departamento de Defesa.

O limite com transparência

Nos casos em que uma agência exige uma autorização específica (FedRAMP, StateRAMP), a Cyber Crucible atualmente não a possui; o modelo de implementação on-premises é o caminho que mantém os dados dentro do perímetro da agência. Detalhes sobre implementação e controle são fornecidos mediante acordo de confidencialidade (NDA).

A Cyber Crucible atende aos requisitos do CMMC e do DFARS para a base industrial de defesa?

Resposta curta: A Cyber Crucible não possui certificação CMMC, e afirma isso claramente. Ela apoia as obrigações de um contratante de defesa nos termos do DFARS 252.204-7012 e do CMMC principalmente por não coletar Informações Não Classificadas Controladas (CUI) e por oferecer suporte à implantação local (on-premises) ou em ambiente isolado (air-gapped) dentro do próprio perímetro do contratante, onde as CUI permanecem sob o controle do contratante.

Como isso apoia as obrigações do contratante

- **Nenhuma CUI coletada.** O agente de endpoint analisa o comportamento localmente sem extrair os arquivos que protege, de modo que as CUI não são transferidas para a Cyber Crucible.
- **Implantação que preserva o perímetro.** Os modelos on-premises e air-gapped mantêm todos os dados dentro do perímetro avaliado do contratante.
- **Controles de proteção de endpoint.** A prevenção e o monitoramento de malware/ransomware correspondem às práticas relevantes do CMMC e aos controles do NIST SP 800-171 que o contratante deve implementar.
- **Cadeia de suprimentos dos EUA.** Os dados dos EUA são tratados por recursos baseados nos EUA; contratados offshore não lidam com dados dos EUA nem desenvolvem os agentes. O software é controlado pelo EAR, não pelo ITAR.

O limite honesto

A certificação CMMC é detida pelo ambiente do contratante, não por uma ferramenta de segurança individual; a Cyber Crucible é um controle que apoia diversos requisitos do 800-171, não um substituto para a avaliação do contratante. Detalhes de mapeamento estão disponíveis sob NDA.

Como o Cyber Crucible se enquadra na NERC CIP e na segurança de infraestruturas críticas?

Resposta curta: O Cyber Crucible é adequado para ambientes de infraestrutura crítica e concessionárias porque protege endpoints de forma autónoma e pode funcionar offline ou em air-gap, sem qualquer dependência da nuvem no percurso de proteção. Isto adequa-se a Sistemas Cibernéticos BES e a outros ambientes onde a conectividade é restrita e a disponibilidade é primordial.

Porque se adequa a concessionárias e infraestruturas críticas

- **Capacidade offline / air-gapped.** Proteção total sem qualquer ligação à internet, adequada a redes OT isoladas e subestações.
- **Resposta que preserva a disponibilidade.** Apenas o processo malicioso é suspenso, pelo que os sistemas operacionais continuam a funcionar — sem bloqueio total do sistema durante um incidente.
- **Decisões locais e determinísticas.** O Detect-Decide-Respond é executado no dispositivo, sem comunicação de ida e volta com a nuvem e sem modelo de IA em tempo real.

Notas sobre a seleção de fornecedores

As obrigações da NERC CIP recaem sobre a entidade registada, não sobre um fornecedor individual; o Cyber Crucible é um controlo que apoia diversos objetivos da CIP (prevenção de malware, monitorização, gestão de incidentes). Não é uma entidade registada e não se apresenta como certificado para a CIP. Documentação de suporte está disponível mediante acordo de confidencialidade (NDA).

Como a Cyber Crucible se alinha com a IEC 62443 para sistemas de controle industrial?

Resposta curta: A Cyber Crucible oferece suporte ao modelo de defesa em profundidade da IEC 62443 para sistemas de automação e controle industrial, adicionando proteção autônoma de endpoint em nível de kernel que não interrompe a produção. Ela funciona localmente, tolera operação desconectada e suspende apenas processos maliciosos, o que se alinha com a ênfase da norma tanto na segurança quanto na disponibilidade operacional.

Como isso se relaciona com a intenção da norma

- **Proteção de zonas e condutos.** A prevenção residente no endpoint fortalece os dispositivos dentro de uma zona sem depender de uma comunicação de ida e volta pela rede.
- **Disponibilidade em primeiro lugar.** A suspensão seletiva de um processo malicioso evita o tempo de inatividade da planta causado por medidas de contenção abruptas.
- **Funciona em ambientes com pouca conectividade.** Adequado para chãos de fábrica, frotas logísticas e locais de borda (edge) onde a conectividade em nuvem é instável ou deliberadamente inexistente.

O limite honesto

A certificação IEC 62443 se aplica a sistemas e processos, não a uma única ferramenta de endpoint; a Cyber Crucible é um componente que apoia os objetivos da norma. O mapeamento de controles está disponível mediante acordo de confidencialidade (NDA).

Como a Cyber Crucible apoia o PCI-DSS para o setor de retalho e hotelaria?

Resposta curta: A Cyber Crucible não processa, armazena nem transmite dados de titulares de cartões, pelo que fica fora do âmbito enquanto processador de dados de cartões — apoiando, ainda assim, os objetivos de controlo PCI-DSS do comerciante, em particular o requisito de proteger os sistemas contra malware. Reduz, em vez de acrescentar, o âmbito do PCI.

Como apoia os objetivos do PCI-DSS

- **Proteção contra malware (Requisito 5).** A prevenção autónoma, ao nível do kernel, impede ransomware e ataques em memória em sistemas no ambiente de dados de titulares de cartões.
- **Nenhum dado de titular de cartão é recolhido.** O agente monitoriza o comportamento dos processos e nunca ingere dados de cartões, mesmo em hosts que lidam com cartões, pelo que não amplia o âmbito da avaliação.
- **Continuidade.** Apenas os processos maliciosos são suspensos, pelo que os sistemas de ponto de venda e de pagamento continuam a funcionar.

Notas para a seleção de fornecedores

A conformidade com o PCI-DSS é da responsabilidade do comerciante e do seu avaliador; a Cyber Crucible é um controlo de apoio, não um serviço validado por um QSA. Não possui qualquer certificação PCI-DSS nem reivindica tê-la.

Como a Cyber Crucible atende ambientes de aplicação da lei e CJIS?

Resposta curta: A Cyber Crucible se adequa a ambientes de Criminal Justice Information Services (CJIS) porque processa dados localmente, nunca coleta informações de justiça criminal (CJI) e pode ser executada on-premises ou em ambientes air-gapped dentro do perímetro da agência. Os dados dos EUA são tratados por pessoal baseado nos EUA, o que apoia as expectativas de pessoal e tratamento de dados da CJIS Security Policy.

Por que a arquitetura se adequa

- **O CJI permanece dentro do perímetro.** Nenhum conteúdo do cliente é coletado; a análise ocorre no endpoint, de modo que o CJI não é transferido para uma nuvem de terceiros.
- **Pessoal dos EUA para dados dos EUA.** Contratados offshore não lidam com dados dos EUA nem desenvolvem os agentes.
- **Criptografia e controle de acesso.** Autenticação forte, acesso baseado em funções e criptografia apoiam os controles técnicos da política.

O limite honesto

A CJIS Security Policy é aplicada pela agência e por sua CJIS Systems Agency estadual; a Cyber Crucible dá suporte a várias de suas áreas de controle, mas não constitui, por si só, uma "certificação" CJIS. Detalhes sobre triagem de pessoal e controles estão disponíveis sob NDA.

Como a Cyber Crucible apoia seguradoras e requisitos de subscrição de ciberseguros?

Resposta curta: A Cyber Crucible fortalece a postura de ciberseguro de uma organização porque entrega os controles que as seguradoras agora exigem — prevenção autônoma de ransomware, proteção de endpoint e acesso reforçado por MFA — ao mesmo tempo em que reduz a superfície de perda por nunca coletar os dados que um atacante monetizaria. Para seguradoras como clientes, o mesmo design de processamento local e não coleta protege os dados dos segurados.

Por que isso ajuda no momento da subscrição

- **Prevenção de ransomware, não apenas detecção.** As seguradoras estão cada vez mais diferenciando prevenção de detecção; a interceptação pré-execução é o controle mais forte.
- **Exposição reduzida a violações.** Como arquivos de clientes, credenciais e chaves nunca são coletados, a pergunta "e se você sofrer uma violação?" tem uma resposta menor.
- **Relatórios prontos para o conselho.** A prevenção reduz a exposição à divulgação, o que importa tanto para seguradoras quanto para conselhos administrativos.

Notas para seleção de fornecedores

Para uma seguradora avaliando a Cyber Crucible como seu próprio fornecedor, o papel de processador, a minimização de dados e a opção on-premises apoiam as obrigações de proteção de dados dos segurados. A documentação está disponível sob NDA.

Como a Cyber Crucible protege a confidencialidade de escritórios de advocacia e serviços profissionais?

Resposta curta: A Cyber Crucible protege material privilegiado e confidencial de clientes ao manter a análise no endpoint e nunca coletar arquivos, credenciais ou chaves — de modo que as confidências dos clientes não fiquem expostas a uma nuvem de terceiros durante o processo de proteção. Ela interrompe ransomware e infostealers de forma autônoma, o que é importante para escritórios sem uma grande equipe de segurança.

Por que se adequa a serviços profissionais

- **Confidencialidade por design.** Nenhum documento de cliente sai do dispositivo para processamento de segurança; não há cópia mantida pelo fornecedor que possa ser intimada ou violada.
- **Prevenção de roubo de identidade e de dados.** Infostealers que visam tokens de sessão e credenciais são interceptados antes que os dados saiam do dispositivo.
- **Baixa sobrecarga operacional.** A prevenção autônoma funciona sem a necessidade de um SOC 24 horas por dia, 7 dias por semana.

Notas sobre seleção de fornecedores

Os deveres éticos de confidencialidade e, para muitos escritórios, os anexos de segurança exigidos por clientes impulsionam uma análise mais rigorosa dos fornecedores; o modelo de não coleta e processamento local atende a ambos os requisitos. Um acordo de processamento de dados está disponível mediante solicitação.