Diligence raisonnable des fournisseurs et confiance en matière de sécurité

Comment Cyber Crucible répond aux questionnaires d'évaluation des risques fournisseurs des entreprises et des institutions financières — ce qu'elle détient et ne détient pas, comment elle soutient les obligations réglementaires, comment l'IA est gouvernée, les niveaux de service, et comment son architecture réduit les risques liés aux tiers. Énoncé clairement et honnêtement.

- Comment Cyber Crucible réduit-il le risque tiers et fournisseurs pour les acheteurs soumis à réglementation ?
- Comment puis-je obtenir le dossier de diligence raisonnable en matière de sécurité de Cyber Crucible ?

Cyber Crucible dispose-t-elle d'un rapport SOC 2 ?

Réponse courte : Non. Cyber Crucible ne détient actuellement pas d'attestation SOC 2, et elle l'indique clairement plutôt que de laisser entendre le contraire. La raison est architecturale : Cyber Crucible est un logiciel s'exécutant localement, et non un dépositaire cloud des données client, de sorte que le modèle SOC 2 d'organisation de service — qui atteste de la manière dont un prestataire stocke, traite et transmet *vos* données sur ses propres systèmes — ne s'applique pas de manière directe à ce cas.

Pourquoi la plupart des clients n'en ont pas exigé

Le SOC 2 atteste des contrôles d'une organisation de service qui détient des données client. La conception de Cyber Crucible élimine ce postulat :

- La détection et la réponse aux menaces s'exécutent sur le point de terminaison, au niveau du noyau, sur l'appareil propre du client.
- Les fichiers, identifiants, clés de chiffrement et jetons de session du client ne sont jamais collectés, transmis ni stockés par Cyber Crucible.
- La plateforme peut être déployée intégralement sur site ou en environnement isolé (air-gapped), au sein de l'infrastructure propre du client.

Étant donné que les catégories de données présentant le plus haut risque ne sont jamais sous la garde de Cyber Crucible, une grande partie de la surface de risque fournisseur qu'un SOC 2 est censé traiter est éliminée de par la conception, plutôt que simplement contrôlée.

Ce qui en tient lieu

Pour les évaluateurs travaillant à partir d'un questionnaire, Cyber Crucible fournit un dossier de sécurité fournisseur préparé qui apporte directement les éléments de preuve des contrôles sous-jacents, et met en correspondance ses contrôles avec les Trust-Service Criteria du SOC 2 et le NIST Cybersecurity Framework afin qu'un évaluateur puisse compléter un questionnaire standard à partir de celui-ci. Ce dossier est disponible sous accord de confidentialité mutuel (NDA) auprès de **dpo@cybercrucible.com**.

La feuille de route en matière d'assurance fait l'objet d'une évaluation continue en fonction des besoins des clients ; cette page sera mise à jour si cette position venait à évoluer.

Cyber Crucible est-il certifié ISO 27001, PCI-DSS, CMMC ou FedRAMP ?

Réponse courte : Non. Cyber Crucible n'a pas obtenu, et ne revendique pas, de certification ou d'autorisation ISO/IEC 27001, PCI-DSS, HIPAA, CMMC ou FedRAMP. Cette précision est indiquée directement, car revendiquer une certification qu'un fournisseur ne détient pas est exactement le type d'incohérence qui compromet la confiance lors d'une revue de diligence raisonnable.

Ce que cela signifie en pratique

- **PCI-DSS :** Cyber Crucible ne traite, ne stocke ni ne transmet de données de titulaires de cartes ; il est donc hors périmètre en tant que processeur de données de cartes, tout en soutenant les objectifs de contrôle de sécurité des terminaux d'un client.
- **HIPAA :** aucun contenu client n'étant collecté, Cyber Crucible évite de créer une relation de garde de données de santé protégées ; un Business Associate Agreement peut être signé lorsque le client en a besoin.
- **ISO 27001 / CMMC / FedRAMP :** non détenues, et non présentées comme telles.

Ce que Cyber Crucible détient

Une validation indépendante et objective existe là où cela compte le plus — voir *Quelle validation de sécurité indépendante Cyber Crucible possède-t-il ?* Les références à des référentiels mentionnées ailleurs dans cette base de connaissances sont des correspondances issues d'auto-évaluations qui aident un évaluateur à relier les contrôles de Cyber Crucible à une norme qu'il utilise déjà ; il ne s'agit pas d'avis d'audit tiers.

Quelle validation de sécurité indépendante Cyber Crucible possède-t-elle ?

Réponse courte : Les pilotes du noyau Windows de Cyber Crucible sont testés de manière objective et signés cryptographiquement dans le cadre du programme de compatibilité matérielle Windows de Microsoft (WHCP). Il s'agit d'une attestation externe et indépendante de la qualité et de la résistance à la falsification du composant le plus privilégié du produit — le code où l'exactitude importe le plus.

Pourquoi le WHCP est significatif

La majeure partie du marché des solutions de sécurité des postes de travail a évité le développement au niveau du noyau, car il est véritablement difficile et coûteux. Cyber Crucible opère délibérément au niveau du noyau, et soumet ses pilotes au programme de Microsoft afin qu'une partie externe — et non uniquement Cyber Crucible — valide que le code le plus sensible est correct et résistant à la falsification.

- La validation est **strictement limitée au pilote**, et n'est pas présentée comme une certification de l'ensemble du produit.
- Il s'agit d'un test objectif et reproductible plutôt que d'un audit administratif subjectif.

Comment cela s'intègre dans une vision d'ensemble

Pour un évaluateur habitué à rechercher un rapport SOC 2, le WHCP constitue un élément de preuve concret et indépendant qu'un SOC 2 ne fournit pas : une validation directe du composant noyau. Il complète — plutôt qu'il ne remplace — les preuves de contrôle figurant dans le dossier fournisseur préparé par Cyber Crucible.

Comment Cyber Crucible prend-il en charge les exigences GLBA et de fournisseur pour les institutions financières ?

Réponse courte : En tant que fournisseur de services logiciels pour une institution financière, Cyber Crucible soutient les obligations de l'institution au titre des exigences de sauvegarde du GLBA et des directives interagences en matière de sécurité de l'information — principalement en ne collectant jamais les informations personnelles non publiques (NPI) que ces règles visent à protéger. Cyber Crucible est un fournisseur de logiciels, et non une institution financière agréée ; il n'est donc pas lui-même soumis à examen réglementaire. Ses contrôles sont conçus pour être examinables dans le cadre du programme de gestion des risques liés aux tiers de l'institution.

Là où l'architecture fait le travail

- **Aucune NPI collectée.** Le produit s'exécute sur des terminaux qui peuvent traiter des NPI sans les extraire. Il n'existe donc aucune information financière du consommateur que Cyber Crucible pourrait utiliser, partager ou redivulguer, ce qui soutient directement la position relative à la règle de confidentialité du GLBA / Regulation P.
- **Programme de sécurité documenté.** Le contrôle d'accès, le chiffrement, la réponse aux violations et la gestion des changements sont documentés et démontrables — les garanties qu'un programme bancaire recherche chez un fournisseur de services.
- **Preuves de diligence raisonnable disponibles.** Un dossier fournisseur préparé est structuré pour servir de preuve de diligence raisonnable et de surveillance continue, comme l'exigent les directives interagences actuelles en matière de gestion des risques liés aux tiers.

Les limites en toute honnêteté

Cyber Crucible soutient les obligations de conformité d'un client ; il ne rend pas, à lui seul, une organisation conforme, et ceci ne constitue pas un avis juridique. Des détails précis, de qualité probante, sont fournis aux évaluateurs d'une banque sous accord de confidentialité (NDA). Voir également *Cyber Crucible répond-il aux attentes du FFIEC et de la gestion des risques liés aux tiers ?*

Cyber Crucible répond-il aux attentes du FFIEC et à celles de la gestion des risques liés aux tiers ?

Réponse courte : Cyber Crucible est conçu pour être auditable au regard des attentes en matière de sécurité, d'exploitation et de continuité d'activité que les examinateurs appliquent à la technologie bancaire, et son dossier fournisseur préparé est organisé pour servir de preuve de diligence raisonnable dont un établissement financier a besoin en vertu des directives interagences de 2023 sur les relations avec les tiers.

Sur quoi le programme d'une banque peut s'appuyer

- Un niveau de détail des contrôles cartographié selon les domaines des questionnaires standards (SIG, CAIQ) ainsi que selon les critères des services de confiance SOC 2 et le NIST CSF.
- Une validation indépendante des pilotes (WHCP) en tant qu'attestation de qualité externe.
- Une posture de continuité d'activité documentée et testée, avec la propriété importante que la protection des terminaux se poursuit même en cas de panne du backend de gestion.
- Des preuves d'assurance, des informations financières et une liste des sous-traitants disponibles sur demande pour les évaluateurs.

Pourquoi l'architecture réduit le risque lié aux tiers

Le fait le plus utile pour un analyste des risques fournisseurs d'une banque est que Cyber Crucible ne collecte jamais les fichiers, identifiants ou clés des clients. Les données qu'un évaluateur craint de voir mal gérées par un fournisseur ne sont pas sous la garde de Cyber Crucible, et ne peuvent donc pas être mal gérées de ce fait. Il s'agit d'une réduction structurelle du risque, et non d'une simple promesse de bien le gérer.

À quels référentiels de sécurité et de conformité Cyber Crucible s'aligne-t-il ?

Réponse courte : Cyber Crucible aligne ses contrôles sur le NIST Cybersecurity Framework, les familles de contrôles pertinentes du NIST SP 800-53, ainsi que sur les CIS Critical Security Controls, et établit une correspondance avec les critères SOC 2 Trust-Service Criteria par souci de commodité pour l'évaluateur. Il s'agit d'**alignements auto-évalués**, proposés afin qu'un évaluateur puisse relier les contrôles de Cyber Crucible à un référentiel qu'il connaît — et non de certifications ou d'opinions d'audit émanant de tiers.

Alignement, présenté en toute transparence

Référentiel	Statut
NIST Cybersecurity Framework (CSF)	Contrôles auto-cartographiés ; ne constitue pas une certification
Familles de contrôles NIST SP 800-53	Alignés le cas échéant ; ne constitue pas une autorisation
CIS Critical Security Controls	Alignés ; non certifiés
Critères SOC 2 Trust-Service Criteria	Correspondance établie par souci de commodité pour l'évaluateur ; aucun rapport détenu
Microsoft WHCP (pilote)	Détenu — une validation externe et indépendante

Pourquoi le préciser ainsi

Un fournisseur qui énumère des référentiels pour lesquels il n'a jamais été audité incite l'évaluateur à se méfier de toutes ses autres réponses. Cyber Crucible indique clairement ce qui relève d'une certification (WHCP) et ce qui relève d'une correspondance auto-évaluée (le reste), afin que l'évaluateur puisse pondérer chaque élément en conséquence.

Cyber Crucible utilise-t-il l'IA, et s'agit-il d'un grand modèle de langage ?

Réponse courte : Cyber Crucible utilise une IA propriétaire — mais uniquement pendant la phase de développement, pas sur votre terminal, et il ne s'agit pas d'un grand modèle de langage. Son IA génétique est un outil de découverte en phase de conception qui identifie l'ensemble déterministe de variables comportementales indiquant une attaque. Ces résultats deviennent des heuristiques fixes et déterministes au niveau du noyau. En exécution, aucune IA, aucun LLM et aucun modèle adaptatif ne s'exécute sur l'appareil.

Pourquoi c'est une position plus forte, et non plus faible

- **Aucun modèle en exécution signifie aucune dérive.** Le comportement du terminal est déterministe, reproductible et testable — et non probabiliste.
- **Aucune surface d'inférence en direct.** Il n'existe aucun modèle sur l'appareil qu'un attaquant pourrait manipuler ou empoisonner.
- **Aucune donnée client dans un quelconque modèle.** Le contenu client, les identifiants et les clés ne sont jamais utilisés pour entraîner, alimenter ou ajuster un modèle, et aucune donnée client ne quitte le terminal pour un traitement par IA.

Pour un évaluateur d'institution financière ou soumis à réglementation, c'est généralement la réponse en matière d'IA qu'il espère entendre : une capacité sans modèle en direct et opaque prenant des décisions sur le terminal.

Sujets connexes

Consultez *Comment la gouvernance de l'IA est-elle assurée dans le cycle de développement de Cyber Crucible ?* pour savoir comment le travail en phase de conception est contrôlé.

Comment l'IA est-elle gouvernée dans le cycle de vie de développement de Cyber Crucible ?

Réponse brève : Étant donné que l'IA génétique de Cyber Crucible n'est utilisée qu'au moment de la conception, elle est régie par le cycle de vie de développement sécurisé (SDLC) plutôt que comme un système de production en direct. Les travaux de découverte s'effectuent dans un environnement interne contrôlé, leurs résultats sont validés et traduits en heuristiques de noyau déterministes, et les pilotes qui en résultent sont signés de manière indépendante sous Microsoft WHCP avant leur publication.

Le cycle de vie gouverné

Phase	Gouvernance
Conception	Les exigences de sécurité sont définies ; la découverte par IA fait partie de la phase de conception, dans le cadre du SDLC
Découverte	L'IA génétique identifie des variables déterministes révélatrices d'attaques en utilisant uniquement des ensembles de données de recherche internes
Dérivation	Les résultats deviennent des heuristiques de noyau fixes et déterministes — aucun modèle en direct n'est déployé
Validation	Les résultats déterministes sont reproductibles et testables ; les modèles et pilotes sont validés par assurance qualité (QA)
Publication	Les pilotes Windows sont signés WHCP ; les modifications suivent une gestion formelle du changement

Données et intégrité

Aucun contenu client, identifiant ou clé n'est utilisé pour entraîner, alimenter ou ajuster un modèle. Les modèles sont propriétaires et développés en interne, sans dépendance à un modèle tiers.

L'intégrité des modèles est maintenue grâce au contrôle de version, à la validation SDLC/QA et à la signature WHCP ; la confidentialité est assurée par un environnement de développement contrôlé.

Où sont traitées les données de Cyber Crucible — sont-elles stockées dans le cloud ?

Réponse courte : L'analyse des menaces et la réponse s'effectuent localement sur le point de terminaison, et non dans le cloud. Cyber Crucible ne collecte pas les fichiers, identifiants ou clés des clients, et ne stocke pas le contenu des clients chez un fournisseur de cloud public tiers. Le backend de gestion et de reporting fonctionne sur une infrastructure exploitée par Cyber Crucible aux États-Unis, et un déploiement entièrement sur site ou isolé (air-gapped) est disponible pour les organisations nécessitant un flux de données externe nul.

Pourquoi le traitement local est important

- **La décision de protection ne quitte jamais l'appareil.** Detect-Decide-Respond s'exécute dans le noyau sur le point de terminaison, généralement en moins de 200 millisecondes, sans aller-retour vers le cloud dans le chemin critique.
- **Protection indépendante du backend.** Une panne du backend de gestion ne réduit pas la protection du point de terminaison.
- **Choix de déploiement.** Les organisations soumises à des exigences strictes de résidence ou de souveraineté des données peuvent exploiter Cyber Crucible entièrement au sein de leur propre infrastructure sécurisée.

Ce sur quoi un évaluateur peut s'appuyer

Étant donné que le contenu des clients n'est jamais collecté, la question « où vont nos données ? » a une réponse simple pour les catégories les plus à risque : elles ne vont nulle part. Des informations détaillées sur l'infrastructure et les sous-traitants sont fournies aux évaluateurs sous accord de confidentialité (NDA).

Quel est le SLA de disponibilité de service et de support de Cyber Crucible ?

Réponse courte : L'accord de niveau de service (SLA) publié par Cyber Crucible garantit une **disponibilité mensuelle du service de 99,9 %** (hors maintenance planifiée et causes échappant à son contrôle raisonnable), avec un recours défini sous forme de crédit en cas d'indisponibilité. Les délais de réponse du support sont hiérarchisés par niveau de gravité, mesurés depuis la création du ticket via le portail d'assistance.

Délais de réponse du support

Gravité	Description	Réponse
SEV1 — Critique	Service hors service ou affectant gravement la production ; aucune solution de contournement disponible	≤ 2 heures
SEV2 — Majeur	Service dégradé de manière à limiter la protection ou la réponse	≤ 4 heures
SEV3 — Mineur	Service dégradé sans affecter la protection ou la réponse	≤ 12 heures
SEV4 — Mineur	Problème non critique, demande d'information ou amélioration	≤ 48 heures

Où le trouver

L'accord de niveau de service complet est disponible publiquement à l'adresse cybercrucible.com/service-level-agreement, et les tickets d'assistance sont créés sur support.cybercrucible.com. Un délai contractuel engagé pour la notification des violations ou des incidents peut être défini pour les clients soumis à une réglementation.

Remarque concernant la disponibilité

Étant donné que la protection des terminaux s'exécute localement, le taux de disponibilité s'applique à l'infrastructure de gestion et de reporting en arrière-plan. La protection sur l'appareil lui-même continue de fonctionner même si cette infrastructure est temporairement indisponible.

Comment Cyber Crucible gère-t-il la conservation et la suppression des données ?

Réponse courte : Cyber Crucible minimise ce qu'il conserve et ne conserve les données que le temps nécessaire à la fourniture du service. Il ne collecte jamais le contenu, les identifiants ou les clés des clients dès le départ, de sorte que les catégories les plus à risque n'ont rien à conserver. La télémétrie comportementale et les métadonnées de sécurité dérivées sont supprimées selon des calendriers définis, et à la fin d'un contrat, toutes les données associées sont mises à disposition pour suppression, avec confirmation.

Le principe

- **Minimiser d'abord.** Les données les plus sensibles ne sont jamais collectées, de sorte qu'il n'y a rien dans ces catégories à conserver ou à détruire.
- **Conserver selon la finalité.** La télémétrie comportementale et les métadonnées de sécurité ne sont conservées que le temps où elles servent à la détection, aux enquêtes et aux rapports, puis sont supprimées.
- **Supprimer à la sortie.** À la fin du contrat, les données associées sont mises à disposition pour suppression, et Cyber Crucible fournit une confirmation.

Ce qui est documenté

Un processus de destruction documenté couvre à la fois les informations imprimées et électroniques. Les périodes de conservation spécifiques par type de données sont fournies aux évaluateurs sous accord de confidentialité (NDA), et peuvent être renforcées par contrat.

Cyber Crucible dispose-t-il d'un délégué à la protection des données ?

Réponse brève : Oui. Cyber Crucible a engagé un délégué à la protection des données (DPO) sous contrat, disposant d'une expertise transjuridictionnelle couvrant le RGPD UE/Royaume-Uni, le CCPA/CPRA de Californie, la loi HIPAA, la norme PCI-DSS, ainsi que les régimes mondiaux de protection des données, y compris la PDPL saoudienne. Le DPO est joignable via la boîte de réception surveillée **dpo@cybercrucible.com**.

Ce que couvre le DPO

- Le programme de confidentialité et les accords de traitement des données.
- Les évaluations d'impact sur la protection des données et les risques liés aux transferts, y compris les clauses contractuelles types pour les transferts transfrontaliers.
- Les décisions relatives à la notification des violations de données et le soutien aux propres obligations de notification du client.
- Un point de contact compétent pour les questions de confidentialité et de conformité lors du processus d'approvisionnement.

Pourquoi un DPO sous contrat avec une expertise mondiale

Plusieurs régimes non américains — dont la PDPL saoudienne — peuvent être plus restrictifs que la législation américaine actuelle. Faire appel à un DPO maîtrisant à la fois le RGPD, le CCPA/CPRA, la loi HIPAA et les PDPL mondiales permet à Cyber Crucible d'accompagner ses clients selon la norme la plus stricte, ce qui satisfait généralement le niveau minimal américain en tant que sous-ensemble.

Cyber Crucible est-il soumis aux contrôles à l'exportation des États-Unis ?

Réponse courte : Oui — le logiciel de Cyber Crucible est soumis aux Export Administration Regulations (EAR) du Département du Commerce des États-Unis. Il n'est **pas** soumis à l'ITAR et n'est pas administré par le Département d'État. Aucune licence spéciale n'est requise pour fournir le logiciel aux clients, et la classification à l'exportation ainsi que le contrôle des tiers sont gérés dans le cadre du programme de conformité de Cyber Crucible.

Ce que cela signifie pour un acheteur

- **EAR, et non ITAR.** Le produit relève de la juridiction du Département du Commerce, le cadre qui s'applique à la plupart des logiciels commerciaux intégrant du chiffrement — et non du régime des articles de défense.
- **Breveté, et examiné.** La technologie a été brevetée à l'international à la suite d'un examen de l'Office des brevets et des marques des États-Unis (U.S. Patent and Trademark Office), qui a inclus un examen par le Département de la Défense.
- **Aucun obstacle lié à la licence.** La fourniture du logiciel à un client ne nécessite pas de licence d'exportation spéciale.

Les détails relatifs à la classification à l'exportation sont disponibles sur demande pour les évaluateurs.

Comment Cyber Crucible réduit-il le risque tiers et fournisseurs pour les acheteurs soumis à réglementation ?

Réponse courte : en supprimant le risque plutôt qu'en se contentant de le gérer. Les trois faits qui répondent aux questions les plus difficiles en matière de risque fournisseur sont les suivants : Cyber Crucible ne collecte aucun contenu client, aucune information d'identification ni aucune clé ; la protection s'exécute localement et survit à toute panne du backend ; et son IA n'existe qu'en phase de développement, jamais sur votre terminal. Ensemble, ces éléments réduisent considérablement la surface qu'un examen de diligence raisonnable est conçu pour sonder.

Les trois facteurs structurels de réduction du risque

- **Aucun contenu collecté.** Aucun fichier client, aucune information d'identification, aucune clé ne sont jamais collectés. Ce seul fait répond aux questions relatives à la PCI-DSS, aux données confidentielles et au scénario « que se passe-t-il en cas de violation » — les données ne sont tout simplement pas là pour être perdues.
- **Protection indépendante du backend.** Detect-Decide-Respond s'exécute localement, avec un objectif de temps de récupération effectif de zéro sur le terminal. Une panne totale du backend ne réduit pas la protection.
- **IA déterministe.** L'IA n'est utilisée qu'en phase de développement ; des heuristiques déterministes s'exécutent en temps réel. Pas de modèle en direct, pas de dérive, des résultats testables.

Renforcement par des tiers indépendants

Lorsque l'attestation indépendante a du poids, Cyber Crucible met en avant ce qui est réel : la signature de pilotes Microsoft WHCP, et — pour le backend géré — les attestations tierces des fournisseurs d'infrastructure sur lesquels il s'appuie. Ne disposant pas de sa propre certification

SOC 2, ces éléments assument honnêtement cette charge plutôt que d'être survendus.

Comment puis-je obtenir le dossier de diligence raisonnable en matière de sécurité de Cyber Crucible ?

Réponse courte : Demandez-le à **dpo@cybercrucible.com**. Dans le cadre d'un accord de confidentialité mutuel (NDA), Cyber Crucible fournit un dossier de sécurité fournisseur préétabli qui répond aux domaines des questionnaires standards (SIG, CAIQ) et se substitue à un rapport SOC 2 lorsqu'un évaluateur en rechercherait habituellement un.

Ce que comprennent le dossier et ses documents complémentaires

- Un dossier de sécurité et de confiance fournisseur préétabli : architecture, traitement des données, chiffrement, gestion des accès, développement sécurisé, réponse aux incidents, continuité des activités, alignement réglementaire, et une cartographie des cadres de contrôle.
- Des résumés de programme d'une page pour la conformité, l'audit et la gouvernance IA/SDLC.
- Un certificat d'assurance, un formulaire W-9 et des informations financières, disponibles sur demande.
- Des clauses contractuelles types, une évaluation des risques liés au transfert (Transfer Risk Assessment) et un accord de traitement des données (Data Processing Agreement), disponibles sur demande.

Documents publics que vous pouvez consulter dès maintenant

Document	Emplacement
Accord de niveau de service	cybercrucible.com/service-level-agreement

Document	Emplacement
Accord de confidentialité mutuel	cybercrucible.com/mutualNDA
MSA et CLUF	cybercrucible.com/msa-and-eula
Politique de confidentialité	cybercrucible.com/privacy-policy

Tout ce qui va au-delà des accords publics est fourni aux évaluateurs dans le cadre d'un accord de confidentialité (NDA), sous réserve de mesures de confidentialité raisonnables.