Gouvernance des données et souveraineté

Ce que Cyber Crucible collecte et ne collecte jamais, comment les données sont protégées en transit, où elles sont traitées, ce qui peut être divulgué dans le cadre d'une procédure judiciaire, et comment les risques liés à la chaîne d'approvisionnement et aux menaces internes sont maîtrisés.

Quelles données Cyber Crucible collecte-t-il — et lesquelles ne collecte-t-il jamais ?

Réponse courte : Cyber Crucible fonctionne selon une directive de Zero-Content Harvesting (absence de collecte de contenu). Il traite la télémétrie opérationnelle du système — chemins d'exécution des processus, chaînes de processus parent-enfant, indicateurs d'exécution matériels et états d'intégrité de la mémoire — analysés localement sur le poste. Il ne collecte, ne transmet, ne stocke ni ne traite les clés de chiffrement, les identifiants, les jetons de session ou vos fichiers.

Catégories strictement exclues

Le logiciel Cyber Crucible ne collecte, ne transmet, ne stocke ni ne traite :

- **Les variables cryptographiques** — clés privées, clés de déchiffrement et clés de chiffrement applicatives.
- **Les identifiants utilisateur** — mots de passe utilisateur, secrets Active Directory et clés privées d'API.
- **Les identifiants de session** — jetons OAuth, jetons d'accès, jetons de rafraîchissement et cookies de session.
- **Les données de contenu client** — fichiers propriétaires, documents, contenus de bases de données, corps d'e-mails et communications des utilisateurs.

Pourquoi une protection complète ne nécessite pas la collecte de contenu

La pleine capacité du logiciel de prévention des menaces est atteinte sans collecter ni exfiltrer le contenu privé des clients. Le moteur comportemental évalue *ce qu'un programme fait* — quels processus atteignent quoi, après avoir fait quoi auparavant — et rien de tout cela ne nécessite d'ouvrir le fichier ou de lire le secret.

C'est le même principe que celui qui sous-tend la protection des identités : l'accès est tracé et analysé sans que l'identifiant lui-même ne soit consulté.

Où l'analyse a lieu

Les chemins d'exécution des processus, la lignée des processus, les indicateurs d'exécution matériels et les états d'intégrité de la mémoire sont analysés **localement sur le poste**. Lorsque l'assistance cloud ou la gestion centralisée est activée, la télémétrie administrative sortante est strictement limitée aux indicateurs opérationnels nécessaires à la surveillance de l'état du système et aux rapports de sécurité.

Quelle est la différence entre la télémétrie système et les données clients ?

Réponse courte : La télémétrie système décrit le comportement d'un logiciel — quel processus en a démarré un autre, à quoi ressemble la mémoire, si les schémas d'exécution sont anormaux. Les données clients sont le contenu que votre entreprise crée et détient — fichiers, e-mails, enregistrements de bases de données, identifiants. Cyber Crucible analyse le premier et ne collecte jamais le second.

Une façon utile d'y penser

La télémétrie est constituée de métadonnées sur le *comportement des machines*. Le contenu, lui, est *l'information elle-même*.

Savoir que le `processus A` a lancé le `processus B`, lequel a ensuite tenté de lire un magasin d'identifiants de navigateur tout en présentant des signes de modification en mémoire, suffit à identifier une attaque. Il n'est pas nécessaire de lire ce qui se trouvait dans ce magasin d'identifiants — et Cyber Crucible ne le fait pas.

Ce que cela signifie concrètement

- L'analyse comportementale est effectuée sur l'accès aux identités **sans traiter les informations d'identité elles-mêmes**.
- La télémétrie qui quitte effectivement le point de terminaison dans les déploiements assistés par le cloud se limite à des indicateurs opérationnels destinés à la surveillance de l'état de fonctionnement et au reporting de sécurité.
- Les métadonnées techniques et comportementales ne sont considérées comme des données personnelles que lorsqu'elles permettent d'identifier directement ou indirectement une personne — et dans ces cas, les identifiants sont pseudonymisés ou masqués.

Contrôle du client

Les sources de télémétrie sont configurables. Les organisations peuvent définir précisément quelles sources sont collectées, afin qu'aucune information superflue ne soit acquise. Les champs qui ne sont pas essentiels à la détection des menaces sont exclus ou supprimés.

Cyber Crucible vend-elle ou partage-t-elle les données des clients avec des tiers ?

Réponse courte : Non. Cyber Crucible ne partage, ne concède sous licence, n'échange ni ne divulgue les informations ou la télémétrie des clients à aucun tiers, et les données des clients ne sont strictement pas à vendre, en aucune circonstance.

Les engagements

- **Zéro partage avec des tiers** — aucun partage, concession de licence, échange ou divulgation des informations ou de la télémétrie des clients à un quelconque tiers.
- **Interdiction de monétisation commerciale** — les données des clients ne sont pas à vendre, en aucune circonstance.
- **Aucun courtage de données d'identité ou de télémétrie** — non échangées, concédées sous licence ou monétisées avec une quelconque partie.

Pourquoi cela est crédible sur le plan architectural

De nombreux fournisseurs font la promesse de ne pas vendre de données. Ce qui distingue celui-ci, c'est qu'une grande partie des éléments sensibles n'est tout simplement pas collectée en premier lieu. Une entreprise qui ne détient jamais vos clés de déchiffrement, vos identifiants ou vos fichiers n'a rien dans ces catégories à vendre, à partager ou à perdre — indépendamment de la politique en vigueur.

Une politique peut changer. Une architecture est plus difficile à inverser.

> Voir aussi : *« Que peut divulguer Cyber Crucible si elle y est contrainte par un gouvernement ou un tribunal ? »*

Que peut divulguer Cyber Crucible si un gouvernement ou un tribunal l'y contraint ?

Réponse courte : Rien dans les catégories qui comptent le plus, car elle ne les détient jamais. Cyber Crucible ne collecte, ne stocke ni ne conserve les clés de déchiffrement, les identifiants des utilisateurs ou les fichiers des clients — il n'existe donc rien de ce type à produire pour une partie privée, un gouvernement ou une puissance étrangère. Comme toute entreprise américaine, elle reste soumise au droit applicable, mais elle ne peut produire des données qu'elle ne détient jamais.

« Rien à divulguer par conception »

Il s'agit d'une position architecturale délibérée plutôt que d'une promesse juridique. Une procédure judiciaire peut contraindre une entreprise à remettre ce qu'elle possède. Elle ne peut pas la contraindre à produire ce qui n'a jamais été collecté.

Comme Cyber Crucible ne collecte ni ne conserve les clés de chiffrement, les identifiants ou les contenus privés, ces catégories sont vides par conception.

Pourquoi cela compte plus qu'avant

Les architectures de sécurité centralisées créent un point d'agrégation de grande valeur. Un fournisseur détenant les clés et les jetons de session de milliers de clients constitue une cible tant pour les cybercriminels que pour les acteurs parrainés par des États — et peut être atteint par voie de contrainte légale, parfois à l'insu du client.

La position de Cyber Crucible en matière de séquestre de clés (key escrow) suit le même raisonnement : elle ne maintient délibérément aucun stockage central des clés, de sorte qu'il n'existe aucun point de défaillance unique à violer ou à assigner en justice.

Une limite énoncée en toute honnêteté

Cyber Crucible est une entreprise américaine et est soumise au droit des États-Unis. L'affirmation ici est étroite et précise : elle ne peut divulguer des données qu'elle ne détient pas. Il s'agit d'une déclaration relative à l'architecture, et non d'une revendication d'immunité face à la procédure

judiciaire.

Comment les données de Cyber Crucible sont-elles protégées en transit ?

Réponse courte : Toutes les communications agent-serveur imposent TLS 1.3. Les charges utiles de données opérationnelles utilisent en outre le chiffrement JSON Web Encryption (JWE) avec des paires de clés cryptographiques uniques par agent, de sorte que les charges utiles ne peuvent être interceptées ni manipulées en transit. L'accès administratif nécessite une authentification par clé ainsi qu'une validation de jeton OAuth 2.0.

Les couches

- **Canaux chiffrés** — toutes les communications agent-serveur imposent TLS 1.3.
- **Chiffrement des charges utiles par agent** — les charges utiles opérationnelles utilisent JWE avec des paires de clés uniques par agent. Comme chaque agent possède sa propre paire de clés, la compromission d'un circuit de transit n'expose pas les autres, et l'interception ou la manipulation en ligne est empêchée.
- **Administration authentifiée** — l'accès au système nécessite une authentification individuelle par clé ainsi qu'une validation de jeton OAuth 2.0, restreignant les actions administratives au personnel autorisé.

Pourquoi les clés par agent sont importantes

Le chiffrement du transport protège uniquement le canal. Le chiffrement des charges utiles par agent protège le *contenu du message* indépendamment du canal — ainsi, un attaquant positionné en ligne, ou un intermédiaire compromis, ne peut toujours pas lire ni altérer ce que l'agent a envoyé.

Infrastructure partagée

Lorsque des environnements de cloud public ou de cloud privé virtuel sont utilisés pour l'administration back-end, Cyber Crucible applique une isolation logique stricte des locataires ainsi

qu'un chiffrement de bout en bout des charges utiles. Les fournisseurs de cloud et les opérateurs d'infrastructure n'ont **aucune visibilité** sur les charges utiles de données opérationnelles ou les états des systèmes des clients.

Où mes données sont-elles traitées, et peuvent-elles rester dans mon pays ?

Réponse courte : Oui. L'infrastructure de Cyber Crucible peut être configurée de sorte que le traitement s'effectue géographiquement à proximité de votre juridiction légale, voire à l'intérieur de celle-ci, et un déploiement entièrement sur site, en air gap, permet de conserver l'ensemble des opérations à l'intérieur de votre propre périmètre réseau, sans aucune télémétrie sortante.

Hébergement souverain

L'infrastructure peut être positionnée de manière à maintenir le traitement à l'intérieur — ou à proximité géographique — de la juridiction légale du client. Ceci est conçu pour faciliter la conformité avec les exigences de résidence des données, notamment le Règlement général sur la protection des données de l'Union européenne (GDPR), la loi saoudienne sur la protection des données personnelles (PDPL), le décret-loi fédéral n° 45/2021 des Émirats arabes unis, et la loi kenyane sur la protection des données (Data Protection Act).

L'option la plus robuste

Pour les organisations nécessitant un isolement total, le modèle sur site exécute l'ensemble du logiciel de gestion backend à l'intérieur de vos propres baies de serveurs physiquement sécurisées. Aucune télémétrie ni aucune donnée ne sortent de votre périmètre réseau souverain.

Étant donné que l'évaluation des menaces et l'interdiction des processus s'effectuent localement sur le terminal, généralement en moins de 200 millisecondes, la protection ne dépend d'aucune connexion externe. La souveraineté ne coûte rien en termes de capacité défensive.

> Voir également : *« Quels modèles de déploiement sont disponibles pour la souveraineté des données ? »*

Quels modèles de déploiement sont disponibles pour la souveraineté des données ?

Réponse brève : Deux. Un modèle sur site entièrement isolé (air-gapped) où aucune donnée ne quitte votre réseau, et un modèle hébergé ou hybride assisté par le cloud avec des communications TLS chiffrées JWE vers des serveurs déployés régionalement. Les deux offrent la même prévention locale en moins de 200 millisecondes.

Comparaison

	Sur site souverain (isolé/air-gapped)	**Hébergé / Hybride assisté par le cloud**
Périmètre de transit des données	Contenu à 100 % au sein des racks de serveurs physiquement sécurisés du client	Communications TLS chiffrées JWE vers des serveurs d'application régionaux
Flux transfrontalier	Aucun flux réseau externe ; aucune télémétrie sortante	Mise en scène géographiquement localisée pour correspondre aux frontières régionales
Conformité réglementaire	Prend en charge les exigences strictes de résidence et de souveraineté nationale des données	Conçu pour s'aligner sur les directives mondiales en matière de confidentialité (GDPR, PDPL, et autres)

Comment choisir entre les deux

Le modèle isolé (air-gapped) convient aux administrations publiques, à la défense, aux infrastructures critiques et à toute organisation soumise à des mandats stricts de résidence nationale ou opérant dans des environnements déconnectés.

Le modèle hybride convient aux organisations qui souhaitent une gestion centralisée et des rapports à l'échelle de l'ensemble du parc tout en conservant les données dans un périmètre régional.

La prévention est identique dans les deux cas. La boucle locale Detect-Decide-Respond s'exécute dans le noyau au niveau du point de terminaison, quel que soit le modèle de

déploiement — seule diffère la localisation de l'infrastructure de gestion et de reporting.

Comment Cyber Crucible gère-t-il les risques liés à la chaîne d'approvisionnement et aux menaces internes ?

Réponse courte : Grâce à des accords de non-divulgation mutuels contraignants pour l'ensemble du personnel disposant d'un accès potentiel, à un accès administratif strictement limité au besoin d'en connaître et réservé au personnel habilité, ainsi qu'à un mandat de tolérance zéro visant à isoler ou à mettre fin immédiatement à toute relation avec un fournisseur, prestataire, sous-traitant ou employé présentant un risque pour les clients ou leur propriété intellectuelle.

Les contrôles

- **Accords de non-divulgation obligatoires** — l'ensemble du personnel disposant d'un accès potentiel aux données opérationnelles des clients ou aux systèmes de gestion est légalement lié par un accord de non-divulgation mutuel avant toute prise de fonction.
- **Accès strict selon le besoin d'en connaître** — l'accès administratif aux instances de gestion des clients est réservé exclusivement au personnel habilité, et uniquement lorsque cela est nécessaire à l'accomplissement d'une opération commerciale ou de support validée.
- **Mandat de désengagement des fournisseurs et ressources** — si un fournisseur, un éditeur de logiciel, un sous-traitant ou un employé présente un risque de sécurité, de confidentialité ou de propriété intellectuelle pour les clients, Cyber Crucible gère activement et isole ce risque, ou met fin immédiatement à la relation avec la ressource concernée.

Pourquoi les risques internes et ceux liés à la chaîne d'approvisionnement sont liés

Il s'agit du même problème envisagé sous deux angles différents : une personne disposant d'un accès légitime devenant le vecteur du risque. Pour le maîtriser, il faut limiter qui dispose d'un

accès, lier ces personnes par contrat, et être prêt à rompre rapidement une relation dès qu'un risque apparaît — y compris une relation commerciale.

Le mandat de désengagement est l'élément qui fait le plus souvent défaut aux organisations. Les contrats et les accords de non-divulgation établissent des obligations ; c'est la volonté de mettre fin immédiatement à une relation avec un fournisseur qui leur donne tout leur sens.

Cyber Crucible intègre-t-il des bibliothèques tierces ou du code étranger ?

Réponse courte : Non. Les capteurs du noyau, les pilotes et les modèles comportementaux Genetic AI sont conçus en interne. Aucun SDK parrainé par un État étranger, aucune bibliothèque tierce non vérifiée, ni aucun mouchard de télémétrie caché n'est intégré au logiciel. Les pilotes du noyau Windows sont soumis à la certification dans le cadre du programme de compatibilité matérielle Windows de Microsoft (Windows Hardware Compatibility Program, WHCP).

L'avantage concurrentiel de l'ingénierie

Développer des capteurs du noyau et des modèles comportementaux en interne est coûteux et long. La plupart des fournisseurs assemblent des composants à la place. C'est précisément dans cet assemblage que le risque lié à la chaîne d'approvisionnement s'introduit dans un produit de sécurité — l'outil disposant des privilèges système les plus étendus est aussi celui où une dépendance non vérifiée peut causer le plus de dommages.

Les composants de Cyber Crucible sont propriétaires et maintenus en interne, ce qui élimine cette catégorie d'exposition plutôt que de simplement la gérer.

Validation externe

Tous les pilotes du noyau Windows font l'objet de tests internes d'assurance qualité et sont soumis à la certification dans le cadre du programme de compatibilité matérielle Windows de Microsoft (Windows Hardware Compatibility Program, WHCP) — une validation indépendante de la qualité et de la résistance à la falsification pour le code s'exécutant au niveau du noyau.

Aucune télémétrie cachée

Il n'existe aucun mouchard de télémétrie caché. Ce que le logiciel collecte est documenté, et les catégories qu'il ne collecte jamais sont explicitement énumérées.

Que signifie la neutralité géopolitique dans un logiciel de sécurité ?

Réponse courte : cela signifie que le logiciel est conçu pour protéger votre organisation sans intégrer de portes dérobées stratégiques étrangères, de partenariats avec des services de renseignement d'États étrangers, ni de dépendance obligatoire au cloud — de sorte que son utilisation n'importe pas les intérêts stratégiques d'un autre pays dans votre infrastructure.

Le problème auquel cela répond

Les outils de sécurité traditionnels reposent souvent sur des modèles centralisés de collecte de données via le cloud, qui exfiltrent en continu la télémétrie des terminaux, les détails des comptes et les artefacts du système de fichiers à travers les frontières nationales et géopolitiques. Cela est lent face aux attaques se déroulant à la vitesse machine, et cela crée une exposition en matière de conformité et de sécurité au regard du RGPD, de la loi saoudienne PDPL, du décret-loi fédéral n° 45/2021 des Émirats arabes unis, et du Kenya Data Protection Act.

Cela soulève également une question que la plupart des processus d'achat ne posent jamais : *dans quelle juridiction ma télémétrie finit-elle par se retrouver, et qui d'autre peut y accéder ?*

Les trois composantes

1. **Aucune porte dérobée stratégique étrangère** — aucun composant de code parrainé par un État ni SDK étranger non vérifié.
2. **Aucun partenariat avec des services de renseignement d'États étrangers** — la télémétrie des clients n'est partagée avec aucun tiers, y compris les gouvernements.
3. **Aucune dépendance obligatoire au cloud** — le logiciel fonctionne entièrement hors ligne, de sorte qu'aucune donnée n'a jamais besoin de traverser une frontière pour que le produit fonctionne.

Le troisième point est ce qui rend les deux premiers applicables de manière crédible. Un produit qui *nécessite* une connexion cloud ne peut pas promettre de manière crédible que vos données restent en place.