

Conformité et risque

Comment la prévention autonome sur l'appareil affecte les obligations réglementaires, la divulgation des violations, la souveraineté des données, la cyberassurance et le reporting des risques au niveau du conseil d'administration.

- [Cyber Crucible collecte-t-elle les clés de chiffrement ?](#)
- [Si une attaque est prévenue, devons-nous quand même signaler une violation ?](#)
- [Comment Cyber Crucible favorise-t-il la conformité HIPAA dans le secteur de la santé ?](#)
- [Comment Cyber Crucible facilite-t-il la conformité FERPA et la protection des données des étudiants ?](#)
- [Que signifie la souveraineté des données pour les déploiements de Cyber Crucible ?](#)
- [Quel risque de conformité l'entierement des clés de chiffrement crée-t-il, et pourquoi Cyber Crucible ne le pratique-t-il pas ?](#)
- [Comment la prévention autonome affecte-t-elle la cyberassurance et le reporting au conseil d'administration ?](#)

Cyber Crucible collecte-t-elle les clés de chiffrement ?

La réponse la plus courte est : « Non. »

Il fut un temps où le logiciel de Cyber Crucible n'arrêtait pas le chiffrement des rançongiciels avant qu'il ne se produise. Il collectait plutôt des clés de chiffrement ou des paramètres possibles, puis utilisait diverses techniques pour déterminer le bon ensemble de déchiffrement (clés incluses) afin de déchiffrer après une attaque de rançongiciel.

Du point de vue de ce que nous collections, une bonne analogie serait une caméra vidéo qui prendrait des photos de tout ce qui pourrait constituer une clé d'un casier. Ensuite, un serveur effectuerait les divers calculs pour déterminer la clé et les paramètres appropriés pour le bon fichier. Les informaticiens appelleraient cela de l'apprentissage automatique.

Avant de passer à autre chose que l'ancien modèle logiciel « collecter tout ce qui pourrait être une clé », nous organisions automatiquement des milliers de clés et de paramètres de chiffrement par machine lors des attaques.

Le module logiciel d'analyse cryptographique a désormais évolué vers un module analytique comportemental supplémentaire, utilisé comme une source de données parmi d'autres pour déterminer si un logiciel tente d'accéder de manière inappropriée à des données d'identité ou à des « données de données » dans le but de les voler ou de les chiffrer.

Si une attaque est prévenue, devons-nous quand même signaler une violation ?

Réponse courte : Généralement, non. Lorsqu'une attaque est arrêtée avant son exécution et qu'aucune donnée n'est consultée, modifiée ou exfiltrée, il n'y a généralement aucune violation à divulguer. Les obligations de divulgation sont habituellement déclenchées par un accès non autorisé à des données protégées — et non par une tentative ayant échoué.

Un exemple concret

Dans le déploiement du secteur des services financiers où Cyber Crucible a intercepté près de 10 000 processus malveillants, le résultat pour le RSSI n'a impliqué aucune divulgation réglementaire. Étant donné que les attaques ont été arrêtées avant leur exécution et qu'aucune donnée n'a été touchée, il n'y a eu aucune notification requise aux clients, aux fournisseurs ou aux régulateurs gouvernementaux — et aucune couverture médiatique, ce qui a préservé la confiance des clients.

Une mise en garde importante

Les exigences de divulgation varient selon la juridiction, le secteur d'activité et le contrat, et les faits spécifiques d'un incident ont leur importance. Cyber Crucible n'est pas un cabinet d'avocats et ceci ne constitue pas un avis juridique. Le principe fiable est que la prévention réduit considérablement votre exposition en matière de divulgation par rapport à une détection après coup — mais c'est à votre conseiller juridique et à votre équipe de conformité de déterminer la marche à suivre pour chaque événement donné.

Comment Cyber Crucible favorise-t-il la conformité HIPAA dans le secteur de la santé ?

Réponse courte : L'ensemble de l'analyse s'effectue localement au niveau du noyau, de sorte que les informations de santé protégées ne quittent jamais le terminal à des fins de traitement de sécurité. Cela évite les risques d'exposition liés à HIPAA que créent les outils de sécurité qui transfèrent des fichiers ou des clés sensibles vers des clouds tiers, et permet de stopper les attaques sans mettre hors ligne les systèmes cliniques.

Le problème posé par la sécurité hébergée chez un fournisseur

De nombreux dispositifs de SOC et de MDR hébergés par des fournisseurs exigent le transfert de clés, de fichiers ou de télémétrie sensibles vers des bases de données cloud tierces. Pour une entité couverte, cela crée un risque de conformité réel et augmente le nombre de parties ayant accès aux données protégées.

Analyse locale, données locales

Cyber Crucible effectue son analyse directement sur le terminal. Les actifs sensibles ne quittent jamais le périmètre sécurisé de l'appareil — ce qui garantit à la fois la souveraineté des données et la position réglementaire qui en découle.

La continuité des soins est essentielle

Une mesure de confinement qui nécessite d'isoler une machine ou de forcer un redémarrage n'est pas acceptable lorsque la prise en charge des patients en dépend. La suspension sélective du seul processus malveillant permet de neutraliser l'attaque en moins de 200 millisecondes, tandis que les opérations médicales, les dispositifs connectés et les systèmes cliniques continuent de fonctionner.

Comment Cyber Crucible facilite-t-il la conformité FERPA et la protection des données des étudiants ?

Réponse courte : FortressAI vérifie l'accès aux données directement sur l'appareil, afin que les dossiers des étudiants et les données familiales ne puissent pas atteindre accidentellement un outil d'IA public. Cyber Crucible stoppe les rançongiciels de manière autonome, sans nécessiter de centre opérationnel de sécurité (SOC) disponible 24 h/24 et 7 j/7 — une contrainte que la plupart des établissements scolaires ne peuvent pas financer.

Les deux problématiques du secteur éducatif

Les écoles et universités sont des cibles privilégiées des rançongiciels, tout en disposant rarement du budget nécessaire pour assurer une surveillance permanente. Dans le même temps, l'adoption de l'IA en classe a progressé bien plus vite que sa gouvernance.

Répondre aux deux enjeux

- **Rançongiciels sans SOC :** une prévention autonome, au niveau du noyau, stoppe les attaques en moins de 200 millisecondes, sans qu'il soit nécessaire d'embaucher des analystes ni de financer un contrat de surveillance 24 h/24 et 7 j/7.
- **Usage de l'IA conforme à la FERPA :** FortressAI évalue chaque requête directement sur l'appareil, afin que les dossiers scolaires protégés et les données personnelles des familles ne se retrouvent pas dans un système d'IA public — y compris en tant que données d'entraînement.

Cette combinaison protège les étudiants et le personnel sans ajouter de charge informatique significative.

Que signifie la souveraineté des données pour les déploiements de Cyber Crucible ?

Réponse brève : Vos données restent là où vous les placez. L'analyse et l'application des mesures se font au niveau du point de terminaison (endpoint), et Cyber Crucible peut être déployé entièrement sur site — fonctionnant dans des baies de serveurs physiquement sécurisées plutôt que dans un cloud public, sans plateformes tierces, sans accès externe et sans partage de données.

Pourquoi la centralisation des données de sécurité constitue un risque

Les architectures de sécurité qui centralisent des éléments sensibles — clés de chiffrement, jetons de session, données d'identité — créent un point de défaillance unique et une cible de grande valeur, tant pour les attaquants criminels que pour les acteurs soutenus par des États.

Il existe un second risque, moins souvent évoqué : un gouvernement pourrait contraindre l'accès à des données détenues de manière centralisée par le biais d'une assignation classifiée ou d'une lettre de sécurité nationale, à l'insu du client et sans son consentement. Il s'agit là d'une exposition majeure en matière de souveraineté des données, sans aucune transparence.

L'option sur site

Pour les organisations exigeant un contrôle absolu, Cyber Crucible propose une installation entièrement sur site, incluant un déploiement en environnement isolé (air-gapped) ainsi qu'une architecture multi-tenant adaptée à la gestion de plusieurs départements ou agences à partir d'une seule instance sécurisée.

Quel risque de conformité l'entiercement des clés de chiffrement crée-t-il, et pourquoi Cyber Crucible ne le pratique-t-il pas ?

Réponse courte : Le stockage centralisé des clés de chiffrement crée un point de défaillance unique, une cible de grande valeur, et une exposition à une divulgation forcée. L'approche de prévention de Cyber Crucible ne dépend pas de la capture ou de l'entiercement des clés ; il n'existe donc aucun stockage central de clés à sécuriser, à soumettre à une assignation, ou à compromettre.

“ Pour la réponse directe concernant le produit, consultez l'article existant « **Cyber Crucible collecte-t-il les clés de chiffrement ?** » Cette page couvre le raisonnement en matière de conformité et de souveraineté des données qui sous-tend cette réponse.

Pourquoi c'est délibéré

Cyber Crucible a initialement développé et breveté une technologie de capture de clés pour la défense contre les rançongiciels. Dès 2021, les souches de rançongiciels avaient évolué au point de la déjouer — en utilisant des bibliothèques de chiffrement personnalisées, des implémentations uniques à chaque exécution, et des chiffrements de flux immunisés contre la capture de clés. Nous avons présenté publiquement cette cryptanalyse lors de la conférence BSides Pittsburgh en 2021.

Le risque que nous avons choisi de ne pas créer

Au-delà du fait qu'elle ne fonctionne plus, la capture de clés nécessite un stockage centralisé des clés de chiffrement. Cela introduit un point de défaillance unique, une cible de grande valeur, et la possibilité d'une divulgation forcée à l'insu du client.

Empêcher l'attaque avant que le chiffrement ne commence élimine entièrement le besoin de clés — ce qui constitue à la fois une défense plus solide et une surface de conformité réduite.

Comment la prévention autonome affecte-t-elle la cyberassurance et le reporting au conseil d'administration ?

Réponse courte : La prévention change ce que vous rapportez. Au lieu de documenter des incidents, des interruptions d'activité et des coûts de remédiation, vous rapportez des attaques qui ont été stoppées sans interruption d'activité, sans divulgation et sans paiement de rançon.

Ce qui préoccupe réellement le conseil d'administration

Dans le déploiement dans le secteur des services financiers évoqué tout au long de cette base de connaissances, le CISO a pu rapporter quatre résultats :

- **Zéro arrêt d'activité** — les attaques suspendues en mémoire ; les opérations et les transactions légitimes se sont poursuivies.
- **Zéro divulgation réglementaire** — rien n'a été accédé, donc rien ne nécessitait de notification.
- **Zéro dommage médiatique** — pas de gros titres, confiance des clients préservée.
- **Un retour sur investissement solide** — une fraction du coût de la pile technologique existante a accompli le travail que celle-ci n'avait pas réussi à faire.

Concernant les paiements de rançon

Environ 90 % des victimes de ransomware ont payé la rançon en 2023. Les clients de Cyber Crucible n'ont rien payé, car les attaques n'ont pas atteint le stade du chiffrage.

Pour les assureurs

Les souscripteurs demandent de plus en plus quels contrôles préviennent un incident plutôt que quels outils le détectent. Un contrôle autonome, au niveau du noyau, qui fonctionne sans temps de

réponse humain constitue une réponse substantielle — bien que les conditions de couverture soient toujours fixées par votre assureur.