

Preuve et évaluation

Preuves, tests et conseils d'évaluation - résultats documentés, comment mener une preuve de concept pertinente, et les questions à poser à tout fournisseur de solutions de prévention.

- [Cyber Crucible réussit-il les tests de simulation de ransomware ?](#)
- [Cyber Crucible génère-t-il des faux positifs ? Quel est le taux de faux positifs ?](#)
- [Cyber Crucible teste-t-il de manière exhaustive tous les rançongiciels possibles ?](#)
- [Quelles preuves existe-t-il que Cyber Crucible arrête réellement les attaques ?](#)
- [Comment devrions-nous mener une preuve de concept pour un outil de prévention ?](#)
- [Quelles questions devrions-nous poser à tout fournisseur de sécurité des terminaux ?](#)
- [Qu'est-il advenu du modèle du « collecteur passif » de l'industrie de la sécurité ?](#)
- [Pourquoi la prévention fondée sur l'intention génère-t-elle moins de bruit d'alerte que la détection par signatures ?](#)

Cyber Crucible réussit-il les tests de simulation de ransomware ?

La meilleure réponse est... cela dépend de la qualité et de la précision des simulations de ransomware, mais nous n'avons pas vu beaucoup de tests de grande qualité qui correspondent aux véritables outils et comportements d'attaque.

Cyber Crucible examine les schémas comportementaux sous-jacents dans l'accès aux fichiers, les comportements de la mémoire, les comportements des processus et les comportements cryptographiques afin d'identifier et de suspendre les activités d'extorsion de données en lien avec une attaque.

Certaines simulations de logiciels d'extorsion de données ont évolué au fil du temps pour devenir une représentation plus fidèle des attaques réelles.

Nous avons connu des simulations qui semblaient se concentrer sur la vérification des contre-mesures d'extorsion de données divulguées par certains fournisseurs, et non sur les techniques des outils d'extorsion et des attaquants eux-mêmes. On pourrait dire : « Tester la contre-mesure, pas l'attaque ».

En réponse, nous ne fuyons jamais les tests contre l'émulation d'attaquants, les tests d'intrusion ou les outils d'extorsion. Nous attaquons régulièrement notre propre logiciel, et jouons les techniques d'attaquants dont nous avons entendu parler en ligne ou que nous avons trouvées (et stoppées) dans les environnements de nos clients.

Cyber Crucible génère-t-il des faux positifs ? Quel est le taux de faux positifs ?

Cyber Crucible s'efforce d'offrir un environnement produit avec 0 faux positif. Cela dit, il arrive parfois qu'il y ait des faux positifs. Voyons d'où ils proviennent.

Actuellement, le taux de faux positifs est d'environ 1 réponse par mois, pour 1800 déploiements/agents, avec une traçabilité complète des raisons pour lesquelles ces réponses se produisent.

Programme corrompu effectuant des opérations rapides sur des fichiers

Que ce soit intentionnellement ou en raison d'une mauvaise programmation, il arrive parfois que des programmes se corrompent eux-mêmes, ou soient corrompus par d'autres programmes en cours d'exécution. Nous constatons cela fréquemment avec les nouvelles fonctionnalités de grandes suites logicielles, telles que Microsoft Office, ou des logiciels propriétaires développés sur mesure.

Ce qui se passe, c'est que la mémoire du programme est corrompue, ce qui augmente le niveau d'inspection du programme. Si cela est ensuite suivi d'un comportement d'accès aux fichiers s'apparentant à de l'extorsion, Cyber Crucible est contraint de suspendre le programme. Nous devenons de plus en plus efficaces pour identifier les bugs connus, et vous pouvez au moins continuer à exécuter votre programme jusqu'à ce qu'il plante (certains redémarrent automatiquement, d'autres non).

Dans un monde où les attaquants n'utilisent pas le système de fichiers, et détournent plutôt la mémoire des programmes en cours d'exécution, nous devons pécher par excès de prudence.

Cyber Crucible dispose désormais de la capacité de créer une permission, où, si le Programme A, avec les Arguments A, provoque une corruption dans le Programme B, avec les Arguments B - nous

pouvons créer une exclusion temporaire pour :

(Programme A + Arguments A) ouvre (Programme B + Arguments B)

De cette façon, aucun risque supplémentaire n'est présumé quant à l'implication d'un pirate informatique, à moins qu'il n'utilise justement exactement les mêmes arguments.

Un excellent exemple de cela s'est produit lorsque Microsoft a introduit pour la première fois l'ouverture de documents Office depuis leur logiciel de chat de bureau. Cela corrompait le programme Office... à chaque... fois... puis le programme Office se mettait à analyser tous les Documents de la machine environ 25 % du temps. Cela... nécessitait une exclusion.

Si vous rencontrez un plantage, utilisez le bouton d'assistance, et nous vous aiderons à créer une exclusion, jusqu'à ce que l'éditeur corrige le problème.

Programmes de sécurité

Cyber Crucible coexiste très bien avec les programmes de sécurité. Contrairement à ce que pensent la plupart des nouveaux clients, les outils de sécurité plus avancés ont tendance à utiliser des interactions système plus avancées que les programmes antivirus qui utilisent des technologies plus anciennes. En fait, certains outils de sécurité gratuits ou peu coûteux exécutent divers scripts Powershell non sécurisés comme élément clé de leur protection, plutôt que de véritables programmes.

En tant qu'outil de sécurité hautement résilient basé sur le noyau, Cyber Crucible est perçu comme étant plus « bas », ou plus « proche » du matériel que la plupart des autres outils. Cyber Crucible identifie automatiquement les autres outils de sécurité et les ajoute aux modèles comportementaux. Tant que les outils de sécurité ne présentent pas de signes de compromission, ils sont autorisés à fonctionner normalement.

Occasionnellement, un outil de sécurité peut provoquer une instabilité du système, lorsque ses tentatives de désactiver ou d'interférer avec le logiciel Cyber Crucible échouent. Dans ces cas, il est préférable de mettre Cyber Crucible sur liste blanche dans l'autre outil de sécurité, afin de l'empêcher d'essayer (et d'échouer) de désactiver ou d'interférer avec Cyber Crucible.

N'hésitez pas à ouvrir un ticket d'assistance auprès de Cyber Crucible, via le portail web, pour discuter de la question.

Outils administratifs ou de sauvegarde

Dans certaines circonstances, un comportement adapté doit être créé pour un outil administratif ou de sauvegarde, pendant que l'équipe Cyber Crucible développe un modèle comportemental amélioré. Dans ce cas, l'équipe Cyber Crucible aidera à la création d'une exception dans le modèle comportemental, qui isolera le programme ainsi que ses arguments pour une fenêtre d'opportunité extrêmement réduite en cas d'attaque potentielle.

Cyber Crucible teste-t-il de manière exhaustive tous les rançongiciels possibles ?

Cyber Crucible fonctionne à partir d'une modélisation comportementale au niveau du noyau, afin de découvrir très rapidement les comportements de vol de données, de vol d'identifiants et de chiffrement par rançongiciel. Les décisions comportementales sont prises à partir d'informations issues du comportement des processus, de comportements dérivés de la mémoire, et de certains types de comportements issus de fichiers, afin de prendre une décision au moment même où l'extorsion est sur le point de se produire.

Malgré le très grand nombre d'échantillons de logiciels de rançongiciel et d'extorsion, ceux-ci peuvent être classés, sur le plan comportemental, en un nombre relativement restreint d'ensembles.

En surface, cependant, les défenses « superficielles » utilisées par une variété d'outils de sécurité doivent contrer un très grand nombre d'outils d'extorsion. Il est important de comprendre que nos analyses comportementales vont beaucoup plus en profondeur dans les outils et les méthodes des attaquants, ce qui réduit considérablement le besoin d'un type de test (impossible) exhaustif de tous les logiciels malveillants possibles, en permanence.

Les développeurs de Cyber Crucible classifient les comportements au niveau du noyau relatifs à la mémoire, aux processus et aux fichiers d'un outil d'extorsion, puis s'assurent qu'il correspond à l'une des capacités défensives connues. Occasionnellement, à l'image d'un vaccin, la formule peut être légèrement ajustée afin de produire une réponse plus précise.

Il est très rare que quelque chose de complètement nouveau apparaisse.

L'équipe de Cyber Crucible travaille de manière exhaustive pour découvrir de manière préventive des techniques nouvelles qui n'ont pas encore été observées au sein de notre clientèle, ni dans le renseignement sur les menaces.

L'effet ?

1. La défense contre les outils d'extorsion de Cyber Crucible est complète contre toutes les variantes connues de rançongiciels.

2. Les nouvelles variantes de rançongiciels sont bloquées avant même d'atteindre les premiers clients. Nous ne savons même pas comment nommer la plupart des logiciels contre lesquels nous

nous défendons pendant environ 120 jours, jusqu'à ce que les chercheurs « rattrapent leur retard ».

3. Les développeurs de rançongiciels et d'outils d'extorsion nous appellent parfois pour voir ce que nous préparons, afin de tenter de trouver un angle d'attaque. Malheureusement, la frustration causée par notre présence semble parfois stimuler leur évolution, ce qui rend d'autres outils encore moins efficaces.

4. Nous accueillons favorablement les tests de notre logiciel. Lorsque des testeurs d'intrusion, des analystes de logiciels malveillants ou des professionnels de l'émulation d'adversaires entament le processus commercial, cela nous enthousiasme !

Quelles preuves existe-t-il que Cyber Crucible arrête réellement les attaques ?

Réponse courte : des déploiements clients documentés, des tests indépendants menés par un grand cabinet d'expertise comptable et de conseil, et de multiples cas où des attaques zero-day ont été stoppées des mois avant que d'autres éditeurs ne les signalent.

Résultats documentés

- **Services financiers :** près de 10 000 processus malveillants interceptés de manière autonome en 60 jours, dont 98 % sur une ferme de serveurs Microsoft SQL hautement privilégiée — sans aucune alerte de la part de trois EDR déployés, d'un MDR, ni d'un SOC externalisé classé parmi les 50 meilleurs.
- **Tests indépendants :** l'un des plus grands cabinets d'expertise comptable et de conseil d'Amérique du Nord a soumis Cyber Crucible à sa propre évaluation face à des scénarios de ransomware, de vol de données et de fraude d'identité.
- **En avance sur le secteur :** Cyber Crucible a stoppé plusieurs attaques zero-day sur des réseaux clients jusqu'à 90 jours avant qu'un autre éditeur ne les signale ou n'y réponde.
- **Attaques basées sur le navigateur :** à partir du quatrième trimestre 2023, les réponses automatisées contre les activités de Chrome, Edge et Chromium sont passées de zéro à plusieurs milliers, avec des CVE associées publiées ultérieurement par Google et Microsoft.
- **Paielements de rançon :** environ 90 % des victimes de ransomware ont payé en 2023. Les clients de Cyber Crucible ont payé 0 \$.

Résilience face à une attaque directe

Lors d'un déploiement maritime, les adversaires ont escaladé jusqu'à détourner des identifiants Windows et verrouiller les systèmes au niveau du BIOS lorsque les tentatives conventionnelles ont échoué. Avec deux autres clients, des attaquants incapables de vaincre le moteur de décision du noyau ont tenté à la place de bloquer la notification au client en attaquant la pile réseau du système d'exploitation — et ont échoué, car les communications réseau de Cyber Crucible sont indépendantes du système d'exploitation.

Comment devrions-nous mener une preuve de concept pour un outil de prévention ?

Réponse courte : Déployez-le aux côtés de votre pile existante dans un environnement de production réel et comparez ce que chaque outil détecte. Le résultat le plus instructif n'est pas un test en laboratoire — c'est l'écart entre ce sur quoi vos outils actuels alertent et ce qui est réellement intercepté.

Pourquoi le déploiement en parallèle fonctionne le mieux

L'entreprise de services financiers présentée dans notre étude de cas la mieux documentée a fait exactement cela. Elle n'a rien retiré. Elle a ajouté Cyber Crucible spécifiquement pour découvrir ce que son investissement existant manquait, et a obtenu une réponse définitive en 60 jours.

Que mesurer

- **Les interceptions sur lesquelles votre pile actuelle n'a jamais alerté.** C'est le signal essentiel.
- **Le délai de décision.** La prévention doit s'achever avant que les dégâts ne surviennent, et non avant qu'un ticket ne soit clôturé.
- **La perturbation de l'activité.** Comptez les temps d'arrêt, les redémarrages et les interruptions causées par des faux positifs.
- **Les heures d'analyste consommées.** La prévention autonome doit réduire la charge de travail, et non ajouter une file d'attente.

Une mise en garde concernant les tests en laboratoire

Tester avec des échantillons prélevés dans des bases de données de logiciels malveillants ne mesure souvent que très peu de choses, car les attaquants conçoivent les logiciels malveillants

pour qu'ils restent dormants tant qu'ils ne reçoivent pas un signal de validation provenant d'un serveur de commande et de contrôle en direct qu'ils exploitent toujours. Un échantillon qui ne fait rien dans votre laboratoire ne prouve rien concernant une attaque réelle.

Quelles questions devrions-nous poser à tout fournisseur de sécurité des terminaux ?

Réponse courte : Demandez où les décisions sont prises, ce qui se passe en l'absence de connectivité, de quoi l'outil dépend pour fonctionner, et s'il prévient ou se contente de signaler. Les réponses permettent de distinguer rapidement l'architecture du marketing.

Questions qu'il vaut la peine de poser

1. **Où la décision de protection est-elle prise — sur le terminal ou dans votre cloud ?** Un aller-retour réseau dans le chemin critique ne peut pas rivaliser avec une attaque se déroulant à l'échelle de la milliseconde.
2. **Que se passe-t-il lorsque la machine est hors ligne ou isolée du réseau (air-gapped) ?** Si la protection se dégrade, ce n'est pas qu'elle était locale.
3. **Votre agent dépend-il des bibliothèques système Windows pour fonctionner ?** Si oui, un attaquant qui compromet ces bibliothèques en mémoire peut l'aveugler ou le réduire au silence.
4. **Exigez-vous des signatures ou des flux de renseignement sur les menaces ?** Si oui, la protection est par définition à la traîne par rapport à l'attaquant.
5. **Une réponse nécessite-t-elle une intervention humaine ?** Si oui, le temps de réponse est limité par la biologie humaine.
6. **Stockez-vous nos clés de chiffrement ou téléversez-vous des données sensibles à des fins d'analyse ?** Un stockage centralisé crée une cible et un risque de divulgation forcée.
7. **Quel est votre taux de faux positifs, et que fait réellement une réponse ?** Le verrouillage complet du système comme seule option de confinement est coûteux dans un hôpital ou une usine.

Pourquoi ces questions sont importantes

La plupart des outils de sécurité des terminaux se ressemblent sur une fiche technique. Ces questions font apparaître les décisions architecturales qui déterminent si un outil peut agir à temps — ou s'il peut seulement expliquer, après coup, ce qui s'est passé.

Qu'est-il advenu du modèle du « collecteur passif » de l'industrie de la sécurité ?

Réponse courte : Pendant des années, les éditeurs ont affirmé que le traitement local sur le point de terminaison était obsolète et ont mis en avant des agents légers qui transmettent la télémétrie brute vers des solutions d'analyse dans le cloud. Les attaques modernes en mémoire visant les bibliothèques centrales du système d'exploitation ont mis ce modèle en échec — les agents continuent de fonctionner mais deviennent en réalité aveugles et muets.

Pourquoi ce modèle a été adopté

Il était moins coûteux à mettre en œuvre. L'ingénierie au niveau du noyau est difficile et onéreuse ; l'envoi de la télémétrie vers le cloud permettait aux éditeurs de proposer des logiciels de point de terminaison peu coûteux, de monétiser de vastes réserves de stockage cloud et de mettre en avant leurs capacités d'IA cloud. Le modèle était optimisé pour l'économie du développement, non pour la défense.

Pourquoi ce modèle échoue aujourd'hui

Ces agents dépendent entièrement des composants natifs du système d'exploitation pour fonctionner et collecter des données. Lorsque les attaquants compromettent ces composants en mémoire, l'agent ne plante pas — il continue de fonctionner mais ne signale plus rien, laissant un tableau de bord indiquant que tout va bien alors que des données sont exfiltrées.

Il existe également des cas documentés d'interdiction délibérée : des attaquants, et dans certains cas vérifiés des concurrents cherchant à dissimuler leurs propres failles, exploitent activement ces dépendances de bibliothèques pour forcer l'arrêt ou saboter les défenses des points de terminaison.

L'impasse architecturale

Corriger ce problème exigerait des éditeurs historiques qu'ils abandonnent leurs pipelines de télémétrie axés sur le cloud et reconstruisent leurs solutions autour d'une informatique en périphérie locale, au niveau du noyau — un effort s'étalant sur plusieurs années. Les acquisitions

récentes et les investissements en capital-risque montrent au contraire que l'industrie s'oriente davantage vers l'analyse dans le cloud et les lacs de données centralisés.

Pourquoi la prévention fondée sur l'intention génère-t-elle moins de bruit d'alerte que la détection par signatures ?

Réponse courte : Parce qu'elle pose une question plus ciblée. Les outils basés sur les signatures et l'heuristique déclenchent une alerte dès qu'un élément *ressemble* à un schéma connu comme malveillant, laissant aux humains le soin de démêler le vrai du faux. La prévention fondée sur l'intention se demande si un programme spécifique est, à cet instant précis, en train d'effectuer une action malveillante à un point d'entrée connu de vol de données — une question qui laisse beaucoup moins de place à l'ambiguïté.

“ Pour connaître le taux de faux positifs mesuré de Cyber Crucible, consultez l'article existant « **Avez-vous des faux positifs ? Quel est votre taux de faux positifs ?** ». Cette page explique la raison architecturale pour laquelle le profil de bruit diffère.

Pourquoi le profil de bruit est différent

Les outils basés sur les signatures et l'heuristique génèrent des alertes lorsqu'un élément *ressemble* à un schéma connu comme malveillant, puis s'appuient sur un tri humain pour distinguer le réel de l'accessoire. C'est ce qui produit plus de 100 alertes par terminal et par jour dans de nombreux environnements.

L'évaluation fondée sur l'intention pose une question plus ciblée : ce programme est-il, à cet instant précis, en train d'effectuer une action malveillante à un point d'entrée connu de vol d'identité ou de vol de données ? Cette question laisse beaucoup moins de place à l'ambiguïté.

Ce que cela signifie sur le plan opérationnel

- Les analystes ne perdent pas de temps à traquer des alertes à faible fiabilité.
- Aucun réglage de règles YARA ni chasse manuelle aux menaces n'est nécessaire pour maintenir le bruit à un niveau gérable.
- Comme la réponse suspend uniquement le processus fautif, même une interception incorrecte n'entraîne pas l'arrêt d'un système.

Pour connaître les taux actuels mesurés dans un environnement comme le vôtre, adressez-vous à votre représentant Cyber Crucible — et consultez l'article existant « Avez-vous des faux positifs ? » pour plus de détails au niveau du produit.