

S'agit-il d'un outil de surveillance comme mes autres tableaux de bord de sécurité ?

La réponse est : cela dépend de la manière dont vous et votre organisation souhaitez utiliser l'outil, mais probablement « non ».

Il est important de noter les stratégies de conception produit de Cyber Crucible :

1. La protection doit être hyper-automatisée, et ne doit nécessiter ni soin et attention constants (traitement des alertes), ni ajustements (configuration) de la part des utilisateurs.
2. Pour les équipes de sécurité disposant de ressources plus importantes, la télémétrie précieuse doit leur être accessible, pour des activités avancées de chasse aux menaces, ou pour soutenir les activités de criminalistique et de réponse aux incidents.
3. L'action n° 2 ci-dessus ne doit en aucun cas dégrader la protection mise en place pour l'action n° 1.

Le retour le plus fréquent que nous recevons de la part des directions informatiques est que leurs employés ignoraient que Cyber Crucible les protégeait déjà depuis des semaines.

Nous avons de nombreux utilisateurs qui exploitent l'outil selon trois modalités :

Installer et oublier (comme vos détecteurs de fumée)

De nombreuses organisations ne disposent pas des ressources nécessaires pour avoir des chasseurs de menaces plongeant dans la télémétrie de Cyber Crucible (ou d'un autre outil), mais elles souhaitent que le risque d'extorsion de données soit « retiré de leurs préoccupations ». C'est tout à fait normal, et la Prévention de l'Extorsion de Données de Cyber Crucible est conçue précisément pour cela.

Ces utilisateurs n'ont pas les ressources nécessaires pour consacrer du temps à examiner les flux de données relatifs à l'injection de processus, à la protection des identifiants et à la création de processus.

Par conséquent, nous constatons qu'à moins qu'ils ne répondent à une réponse automatisée rare de Cyber Crucible, ou qu'ils n'effectuent une gestion d'inventaire, comme lorsqu'une nouvelle machine doit se voir déployer Cyber Crucible...

...ils ne se connectent tout simplement pas au portail web de Cyber Crucible, et laissent l'automatisation faire son travail.

C'est tout à fait normal !

Chasse aux menaces avancée + protection automatisée

Les capacités d'[injection de processus](#), de surveillance de l'utilisation des identifiants, et de [création de processus](#) fournissent un ensemble riche de données, capturées via une analyse comportementale au niveau du noyau, pour mener des activités de chasse aux menaces.

La protection automatisée s'active dès que commence le vol de données, le vol d'identifiants (jetons, mots de passe), ou le chiffrement par rançongiciel. Pour tout le reste, il s'agit d'une excellente ressource.

La constatation la plus fréquente jusqu'à présent concerne des outils de gestion à distance non gérés (du moins par les administrateurs informatiques actuels) installés par les utilisateurs. Oui, ils entraînent parfois une protection automatisée contre l'extorsion (c'est-à-dire lorsque l'outil RMM non géré est utilisé par un acteur malveillant), mais il est toujours préférable d'en savoir davantage sur votre environnement au préalable, quoi qu'il en soit !

Voici une courte vidéo d'un type d'attaque que nous avons observé utilisé par des attaquants, dans plusieurs environnements clients, et qui a permis de contourner avec succès les solutions EDR des clients (nous préférons ne pas citer de noms... il s'agissait de trois produits dans quatre entreprises).

[rr-com-dll.mp4](#)

Analyse criminalistique post-incident et remédiation

Il existe plusieurs types de cas d'usage pour les données de Cyber Crucible.

Le premier permet à une personne chargée de la sécurité au sein d'une entreprise, ou à une personne informatique, d'enquêter sur la cause première de la suspension d'un programme. Pour certains clients, qui installent généralement notre logiciel puis ne se reconnectent que lorsqu'il y a de nouveaux employés à intégrer, ils n'ont jamais utilisé aucune fonctionnalité de Cyber Crucible en dehors de la page de gestion des agents. Nous sommes heureux de les aider à découvrir l'[analyse de cause première](#) - qui est simple et sans difficulté pour les utilisateurs techniques et semi-techniques.

Le deuxième type de client pour l'analyse criminalistique post-incident concerne les cabinets de DFIR appelés à enquêter sur un problème chez un client, parfois à la demande de la compagnie d'assurance cyber, et Cyber Crucible est installé après la survenue d'un incident. (Nous ne pouvons pas toujours être présents avant l'attaquant, aussi souhaitable que cela soit... sinon, chaque entreprise au monde nous utiliserait, et l'extorsion appartiendrait au passé !)

La meilleure façon de décrire un déploiement après une attaque par extorsion est « désordonné ». Non pas parce que nous sommes difficiles à installer ou à mettre en service pour la protection. Bien au contraire ! Dans ce cas, les attaquants se sont généralement déplacés dans le système, et sont ancrés dans les systèmes d'exploitation, les équipements réseau, l'Active Directory, et opèrent en mémoire. Plusieurs machines finissent par avoir des processus suspendus, et parfois les attaquants tentent même de reprendre le contrôle. C'est un peu comme prendre un médicament qui vous rend malade au début, mais dont vous avez besoin pour finir par aller mieux.

Les clients déjà sous stress réagissent parfois émotionnellement à « davantage » de bruit, alors même que les attaquants sont enfin débusqués et vaincus. Il faut beaucoup d'explications quant aux raisons ou à la manière dont leurs dispositifs de sécurité en place n'ont pas détecté les attaquants. Au final, cependant, l'entreprise reprend le contrôle de son infrastructure informatique. Ils ne feront pas partie des 80 à 90 % d'entreprises qui sont de nouveau victimes d'extorsion un an ou deux plus tard, dans ce que nous appelons « l'économie de l'abonnement à l'extorsion ».

Le troisième type de client que nous avons est un MSSP qui, souvent partenaire de Cyber Crucible, répond à une protection automatisée de Cyber Crucible. Ils doivent découvrir la manière dont l'attaquant a obtenu un point d'ancrage temporaire, et combler toute faille de sécurité. La bonne nouvelle est que les rapports de conformité HIPAA ou autres font généralement état de peu ou pas d'atteinte à la confidentialité, en raison de la rapidité de la réponse automatisée. Bien souvent, le MSSP rapporte « rien à signaler », ce qui rend toutes les parties concernées satisfaites. Enfin, sauf le criminel.

Revision #1

Created 2026-07-24 06:54:20 UTC by Dennis Underwood

Updated 2026-07-24 06:54:20 UTC by Dennis Underwood