Cyber Crucible est-il un EDR, un XDR, un MDR ? Ou bien quelque chose d'autre, comme une IA agentique ?

Réponse courte : il présente des éléments à la fois d'EDR et de XDR, mais la question de la catégorie n'est pas la bonne. Ce qui compte, c'est *où la décision est prise*. La logique de réponse de Cyber Crucible s'exécute entièrement sur le poste de travail (endpoint), en utilisant uniquement les informations disponibles à cet endroit au moment de l'attaque — car les serveurs d'analyse distants introduisent deux faiblesses fatales : la latence et la fragilité.

La réponse honnête à la question de l'étiquette

- **En tant qu'EDR :** si un EDR utilise la télémétrie du poste de travail pour prendre des décisions, alors la réponse automatisée de Cyber Crucible est un EDR. Elle bloque les comportements d'extorsion en quelques millisecondes, en utilisant uniquement des informations locales.
- **En tant que XDR :** la télémétrie est également envoyée vers une base de données (appliance client ou centralisée) pour la corrélation, la traque des menaces (threat hunting), le travail sur les menaces internes, et les audits informatiques. Selon la définition marketing du XDR, cela répond au critère.

L'équipe est à l'aise avec l'appellation « EDR pour la défense contre l'extorsion », même si l'informatique en périphérie (edge computing) est perçue dans certains cercles comme relevant de la génération précédente. Le raisonnement ci-dessous explique pourquoi ce point de vue est erroné.

Pourquoi l'analyse distante est devenue un handicap — la latence

Le « X » de XDR représente le déplacement de la puissance de calcul analytique vers des serveurs distants. Cela procure de la puissance, mais coûte du temps, et les attaquants ont bâti leur savoir-faire autour de cet écart :

- **Vitesse :** les attaques ont été accélérées de sorte que les actions irréversibles se terminent avant qu'un serveur d'analyse ne puisse répondre. Ceci est particulièrement visible avec des éléments petits mais à forte valeur, comme les mots de passe.
- **Parallélisme :** de nombreux outils de protection des postes de travail inspectent un programme, attendent, puis passent au suivant. Les attaquants exécutent plusieurs programmes d'extorsion à la fois — 5 000 fichiers consultés en parallèle au lieu de 500.
- **Distribution :** l'extorsion s'exécute simultanément sur de nombreuses machines. Cyber Crucible a observé environ 75 machines à la fois. Un outil doit alors faire face à 50 programmes sur 75 machines — soit 3 750 programmes à inspecter.
- **Processus commandants :** certains attaquants exécutent un contrôleur local qui relance instantanément tout outil d'extorsion qui serait arrêté.

Les stratégies de détection et de réponse attendent, par nature, que l'attaque soit déjà en cours. La meilleure analogie consiste à arrêter les braqueurs de banque à la porte plutôt qu'après qu'une certaine quantité d'argent a quitté le coffre-fort.

Pourquoi l'analyse distante est devenue un handicap — la fragilité

Environ 80 % des solutions EDR et XDR nécessitent un accès à des serveurs d'analyse distants pour fonctionner de manière optimale, et sont à peine fonctionnelles sans ce « cerveau » dans le cloud.

Les attaquants exploitent cela directement : en obtenant un accès suffisant pour modifier les règles du pare-feu, ils empêchent l'outil du poste de travail d'atteindre ses serveurs d'analyse, et l'outil perd alors sa capacité à analyser ou à répondre. Il reste non exploité, installé, en cours d'exécution — et presque totalement inefficace.

Ce que Cyber Crucible fait à la place

Parce que la latence et la fragilité rendent la dépendance au cloud intenable pour la défense contre l'extorsion, Cyber Crucible a inventé une capacité de détection et de réponse dont l'analyse comportementale utilise **uniquement les informations disponibles sur le poste de travail au moment de l'attaque**. L'interdiction se produit localement, généralement en moins de 200 millisecondes, sans aller-retour vers le cloud dans le chemin critique.

La télémétrie qui alimente bien la base de données soutient l'investigation plutôt que la protection — traque des menaces, détection des menaces internes, audits informatiques — et une API ouverte

permet de l'intégrer à des plateformes XDR ouvertes, à des outils SOAR ou RPA. Ce travail a de la valeur, mais ce n'est jamais lui qui se dresse entre vous et une attaque en cours.

Revision #1
Created 2026-07-24 06:53:46 UTC by Dennis Underwood
Updated 2026-07-24 06:53:46 UTC by Dennis Underwood