

En quoi Cyber Crucible diffère-t-il des solutions EDR, XDR et MDR ?

Réponse courte : L'EDR, le XDR et le MDR sont des outils de détection et de réponse : ils observent une attaque, génèrent une alerte et s'appuient sur un humain ou un service cloud pour décider de la marche à suivre. Cyber Crucible est un outil de prévention : il décide de manière autonome au niveau du terminal et stoppe le processus malveillant en moins de 200 millisecondes, avant que des dommages ne surviennent.

Les différences concrètes

	EDR / XDR / MDR	Cyber Crucible
Temps de réponse	De quelques minutes à plusieurs heures	Moins de 200 millisecondes
Méthode de détection	Signatures et données historiques	Intention comportementale, sans signatures
Couverture des menaces zero-day	Partielle	Conçu pour les menaces inconnues
Dépendance humaine	Élevée — analystes et SOC	Aucune — entièrement autonome
Où les décisions sont prises	Analytique cloud	Localement, dans le noyau

Pourquoi cet écart est important

Les outils de détection ont été conçus pour une époque où les attaques se déroulaient sur des heures, voire des jours. Les attaques automatisées se déroulent désormais en quelques secondes. Un outil qui produit une alerte précise après l'exfiltration des données a documenté la perte, il ne l'a pas empêchée.

Il ne s'agit pas d'affirmer que la détection n'a aucune valeur — la criminalistique et l'investigation ont leur importance. Il s'agit de reconnaître que la détection seule ne peut pas arrêter une attaque à la vitesse d'une machine.