

# Comment Cyber Crucible m'aide-t-il à gérer les fournisseurs de cybersécurité et les résultats ?

**Réponse courte :** Cyber Crucible gère la prévention automatisée au niveau du terminal, ce qui vous libère pour sélectionner et tenir responsable votre propre fournisseur de surveillance ou de réponse, plutôt que d'être enfermé dans un service groupé et difficile à évaluer, lié à un seul fournisseur d'EDR ou de XDR.

## Le problème caché des services de sécurité groupés

De nombreuses organisations paient des sommes importantes pour un centre d'opérations de sécurité hébergé qui est associé à un produit particulier de détection ou de détection et réponse étendues au niveau des terminaux. Le problème est que cet arrangement laisse souvent le client avec peu de visibilité sur l'attention ou l'efficacité réelle de ce service de surveillance. Vous ne savez peut-être pas à quel point votre environnement est surveillé de près, à quelle vitesse les incidents sont escaladés, ou si vous êtes un compte prioritaire pour ce fournisseur. Comme la surveillance est liée à la technologie sous-jacente, il y a peu de marge de négociation, de mesure ou de remplacement du service s'il ne répond pas aux attentes.

## Séparer la prévention de la surveillance redonne le contrôle

Cyber Crucible se concentre sur la couche de prévention de la protection des terminaux, en arrêtant automatiquement les tentatives de ransomware, de vol de données et d'usurpation d'identité. Comme la prévention est gérée de manière indépendante, les organisations ne sont plus contraintes d'accepter une offre groupée unique pour la détection et la réponse. Au lieu de cela, vous avez la liberté de choisir le partenaire de détection et réponse gérées (MDR) ou de services de sécurité gérés (MSSP) qui répond à vos besoins, qu'il s'agisse de votre propre personnel interne,

d'un MSSP spécialisé, ou d'un tout autre fournisseur de MDR.

# Pourquoi le choix est important

Cette séparation vous donne la possibilité de définir vos propres accords de niveau de service, de mesurer la qualité et la réactivité de l'équipe qui surveille votre environnement, et de tenir ce fournisseur responsable par le biais d'une véritable relation contractuelle. Plutôt que d'espérer qu'un fournisseur groupé vous accorde une attention adéquate, vous pouvez évaluer et faire respecter des normes de performance selon vos propres critères. En fin de compte, l'approche de Cyber Crucible vise à donner aux organisations un contrôle véritable — un contrôle face aux attaquants, et tout aussi important, un contrôle sur les relations avec les fournisseurs et les contrats qui soutiennent leur programme de sécurité.

<https://player.vimeo.com/video/1046829518?texttrack=fr>

[Regarder sur Vimeo](#) · Sous-titres : English, Français, Español, العربية

---

Revision #2

Created 2026-07-24 07:23:15 UTC by Dennis Underwood

Updated 2026-08-06 18:38:41 UTC by Dennis Underwood