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.

Revision #1
Created 2026-07-24 07:03:47 UTC by Dennis Underwood
Updated 2026-07-24 07:03:48 UTC by Dennis Underwood