Comment devrions-nous mener une preuve de concept pour un outil de prévention ?

Réponse courte : Déployez-le aux côtés de votre pile existante dans un environnement de production réel et comparez ce que chaque outil détecte. Le résultat le plus instructif n'est pas un test en laboratoire — c'est l'écart entre ce sur quoi vos outils actuels alertent et ce qui est réellement intercepté.

Pourquoi le déploiement en parallèle fonctionne le mieux

L'entreprise de services financiers présentée dans notre étude de cas la mieux documentée a fait exactement cela. Elle n'a rien retiré. Elle a ajouté Cyber Crucible spécifiquement pour découvrir ce que son investissement existant manquait, et a obtenu une réponse définitive en 60 jours.

Que mesurer

- **Les interceptions sur lesquelles votre pile actuelle n'a jamais alerté.** C'est le signal essentiel.
- **Le délai de décision.** La prévention doit s'achever avant que les dégâts ne surviennent, et non avant qu'un ticket ne soit clôturé.
- **La perturbation de l'activité.** Comptez les temps d'arrêt, les redémarrages et les interruptions causées par des faux positifs.
- **Les heures d'analyste consommées.** La prévention autonome doit réduire la charge de travail, et non ajouter une file d'attente.

Une mise en garde concernant les tests en laboratoire

Tester avec des échantillons prélevés dans des bases de données de logiciels malveillants ne mesure souvent que très peu de choses, car les attaquants conçoivent les logiciels malveillants pour qu'ils restent dormants tant qu'ils ne reçoivent pas un signal de validation provenant d'un

serveur de commande et de contrôle en direct qu'ils exploitent toujours. Un échantillon qui ne fait rien dans votre laboratoire ne prouve rien concernant une attaque réelle.

Revision #1
Created 2026-07-24 07:03:16 UTC by Dennis Underwood
Updated 2026-07-24 07:03:16 UTC by Dennis Underwood