Comment la prévention autonome affecte-t-elle la cyberassurance et le reporting au conseil d'administration ?

Réponse courte : La prévention change ce que vous rapportez. Au lieu de documenter des incidents, des interruptions d'activité et des coûts de remédiation, vous rapportez des attaques qui ont été stoppées sans interruption d'activité, sans divulgation et sans paiement de rançon.

Ce qui préoccupe réellement le conseil d'administration

Dans le déploiement dans le secteur des services financiers évoqué tout au long de cette base de connaissances, le CISO a pu rapporter quatre résultats :

- **Zéro arrêt d'activité** — les attaques suspendues en mémoire ; les opérations et les transactions légitimes se sont poursuivies.
- **Zéro divulgation réglementaire** — rien n'a été accédé, donc rien ne nécessitait de notification.
- **Zéro dommage médiatique** — pas de gros titres, confiance des clients préservée.
- **Un retour sur investissement solide** — une fraction du coût de la pile technologique existante a accompli le travail que celle-ci n'avait pas réussi à faire.

Concernant les paiements de rançon

Environ 90 % des victimes de ransomware ont payé la rançon en 2023. Les clients de Cyber Crucible n'ont rien payé, car les attaques n'ont pas atteint le stade du chiffrement.

Pour les assureurs

Les souscripteurs demandent de plus en plus quels contrôles préviennent un incident plutôt que quels outils le détectent. Un contrôle autonome, au niveau du noyau, qui fonctionne sans temps de

réponse humain constitue une réponse substantielle — bien que les conditions de couverture soient toujours fixées par votre assureur.

Revision #1
Created 2026-07-24 07:01:05 UTC by Dennis Underwood
Updated 2026-07-24 07:01:05 UTC by Dennis Underwood