En quoi cela diffère-t-il de la surveillance d’identité classique ?

La fonctionnalité de protection contre le vol d’identité numérique de Cyber Crucible est proactive et préventive. Elle empêche l’accès aux informations nécessaires pour mener des opérations de chantage, d’extorsion et de vol d’identité moderne.

La protection traditionnelle contre le vol d’identité traite des mots de passe et autres données entre les mains de fraudeurs, et surveille des éléments tels que l’utilisation frauduleuse de cartes de crédit, la souscription de prêts frauduleux, ou la découverte éventuelle de mots de passe lors de violations de données. Cette approche est très réactive et difficile à gérer au quotidien pour les clients. Elle ouvre également la voie, comme Cyber Crucible l’a observé, au chantage envers des particuliers, voire à la coercition d’employés et de dirigeants pour qu’ils aident les attaquants à s’en prendre à leurs employeurs.

Les attaquants déploient des efforts concertés pour cibler les cookies, les identifiants de connexion, les plateformes de messagerie et d’autres formes d’authentification et de données privées afin de faciliter leurs attaques.

Les analyses de Cyber Crucible axées sur le vol d’identité empêchent cela, grâce à une prise de décision comportementale faisant autorité, sans intervention de l’utilisateur, face aux tactiques d’extorsion modernes et aux attaques sans fichier menées par des cybercriminels.

Revision #1
Created 2026-07-24 06:50:58 UTC by Dennis Underwood
Updated 2026-07-24 06:50:58 UTC by Dennis Underwood