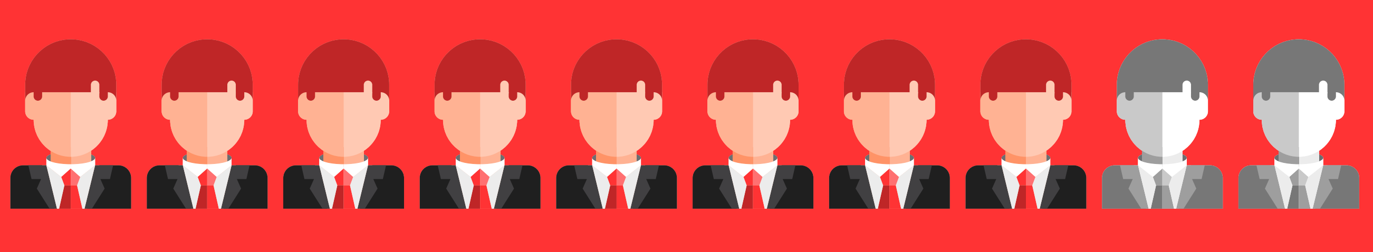
LA DÉTECTION DES CYBER INCIDENTS EN BREF

ALERTE!



79% des équipes de cyber sécurité se sentent dépassées par le nombre trop important d'alertes relatives aux cyber attaques.

Enterprise Management Associates. Une journée dans la vie d'un professionnel de la cyber sécurité (2017).

50 % DES ALERTES SONT DES FAUX POSITIFS

Ponemon Institute. Rapport 2017 sur la sécurité des postes de travail (2017).

Une organisation de taille intermédiaire enregistre en moyenne

UN MILLIARD

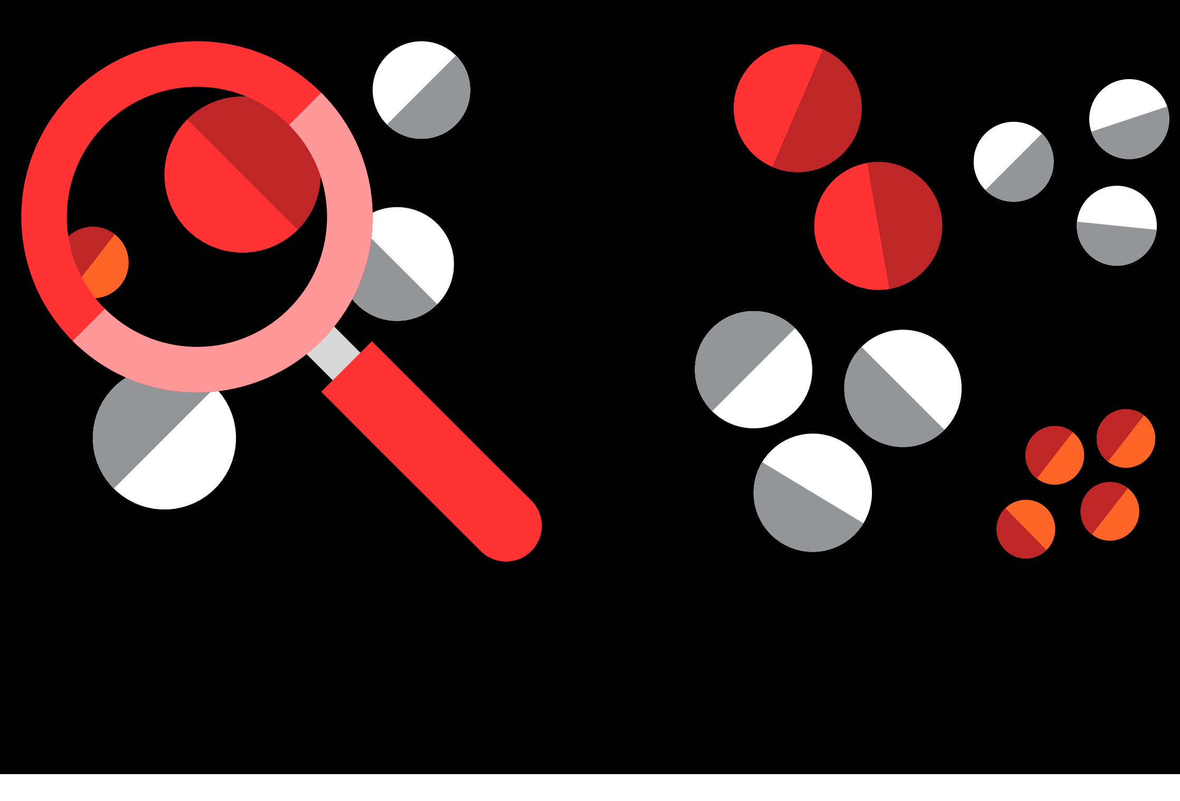
d'évènements chaque mois

Et seulement **10** de ces détections requièrent une action de l'utilisateur

F-Secure. Détection des attaques ciblées grâce à Broad Context Detection™ (2018)

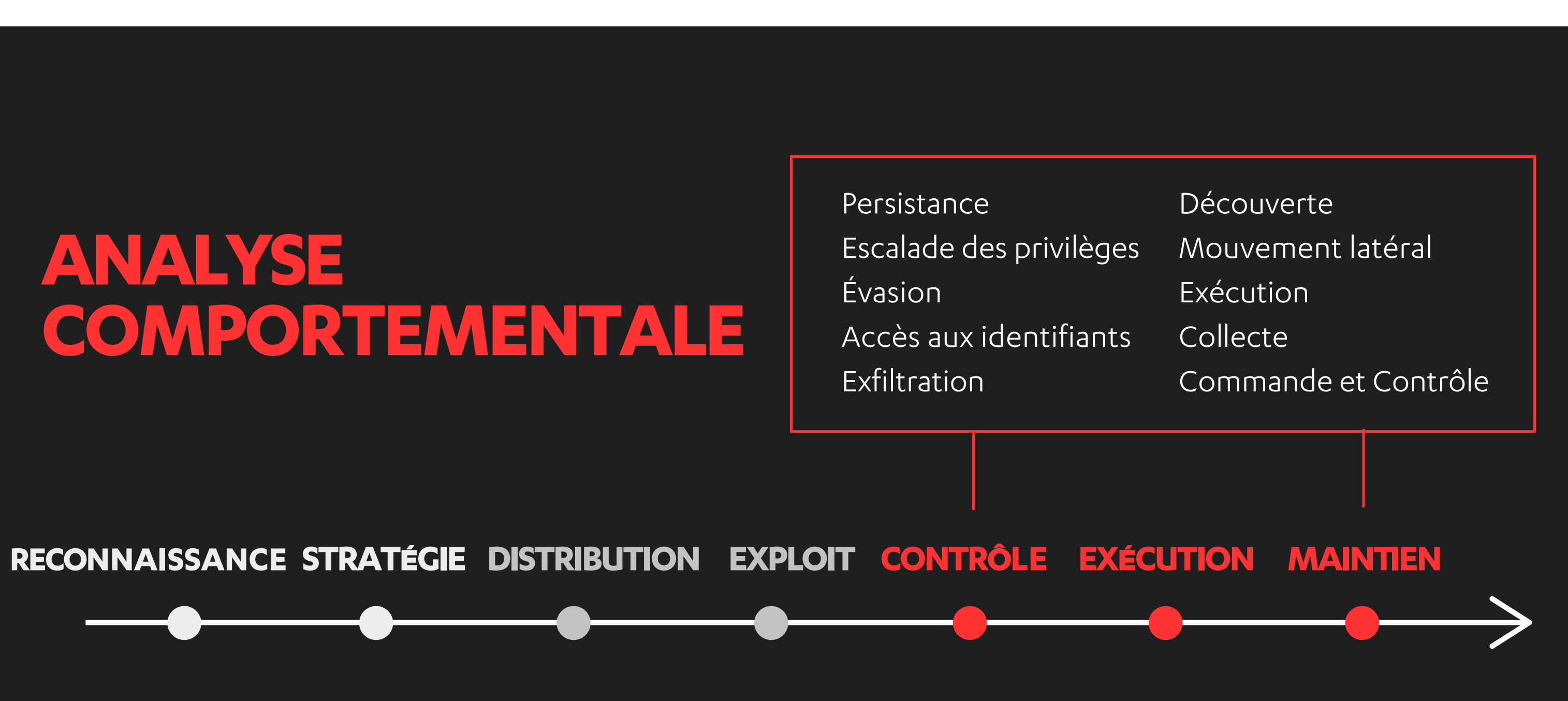
LE CONTEXTE EST LA CLÉ

UN ÉVÈNEMENT ISOLÉ NE PEUT PAS ÊTRE INTERPRÉTÉ SEUL : IL FAUT LE CONTEXTUALISER



BROAD CONTEXT DETECTION™

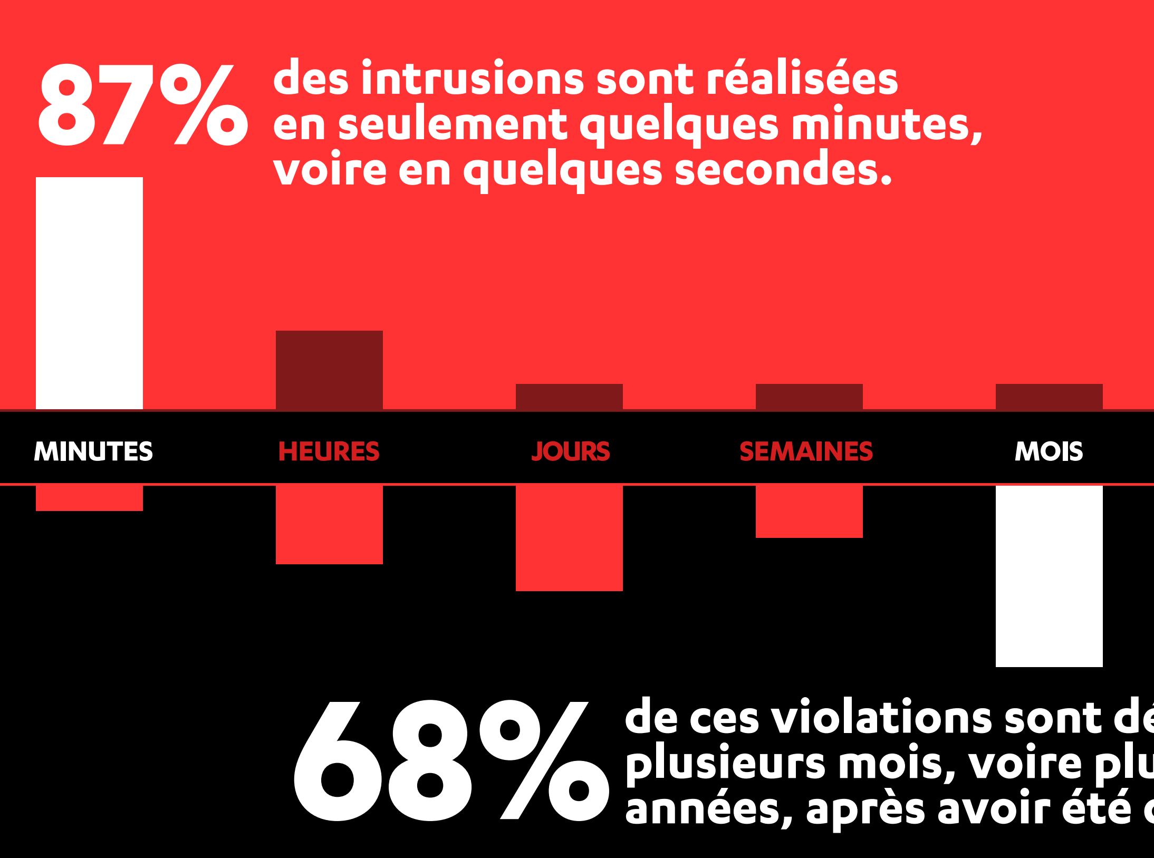
ANALYSE COMPORTEMENTALE



Persistance
Escalade des privilèges
Évasion
Accès aux identifiants
Exfiltration
Découverte
Mouvement latéral
Exécution
Collecte
Commande et Contrôle

ATTAQUE

87% des intrusions sont réalisées en seulement quelques minutes, voire en quelques secondes.



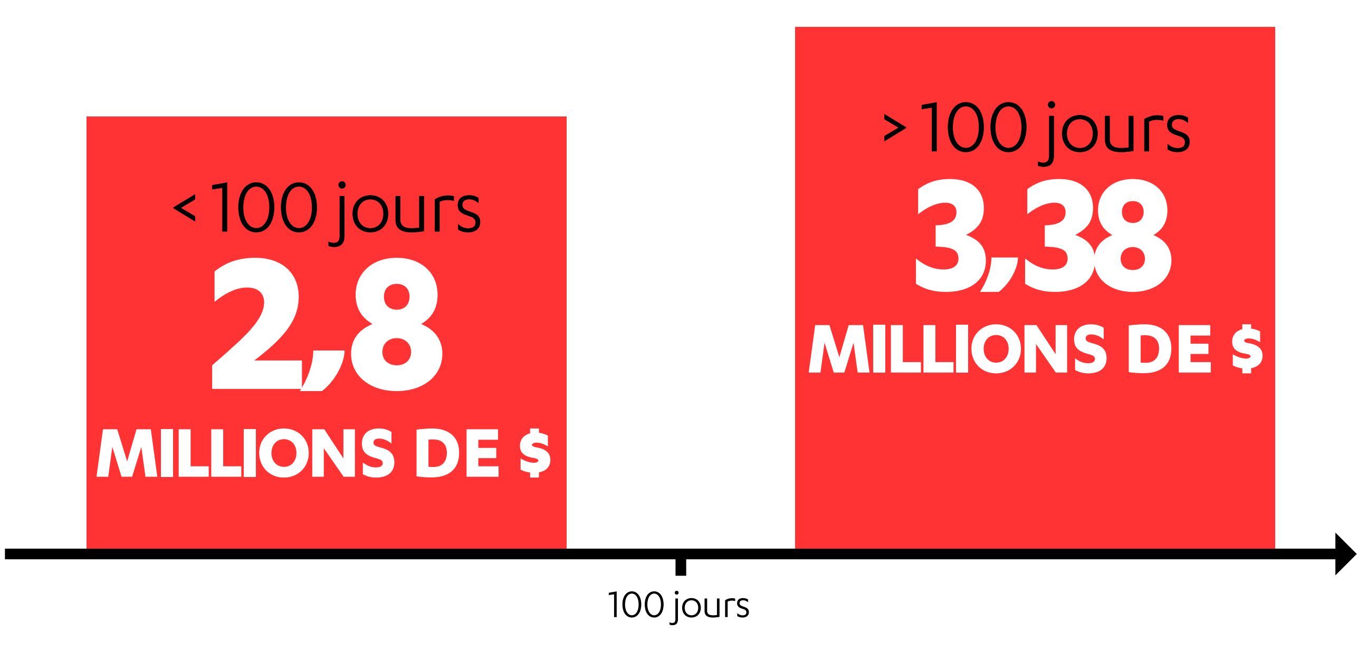
68% de ces violations sont détectées plusieurs mois, voire plusieurs années, après avoir été commises.

DÉTECTION

Verizon. Rapport 2018 sur les violations de données.
11e édition (2018).

LA RAPIDITÉ A SON IMPORTANCE

Plus la violation de données est détectée tardivement, plus les coûts augmentent :



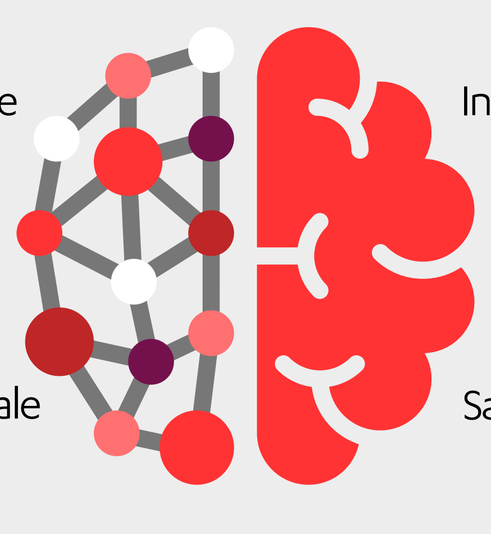
IBM & Ponemon Institute. Étude sur le coût des violations de données en 2017 (2017).

L'HOMME ET LA MACHINE :

Intelligence artificielle

Machine learning

Analyse comportementale



Intelligence humaine

Créativité

Savoir-faire en cyber sécurité

LA COMBINAISON GAGNANTE

AUGMENTEZ VOTRE CAPACITÉ DE DÉTECTION

F-Secure Rapid Detection & Response

F-Secure