GIA SYMPOSIUM MONTRÉAL 2015
GESTION DES IDENTITÉS ET DES ACCÈS

La GRC dans la GIA

Identity Analytics & Intelligence

Une approche pragmatique

BRAINWAVE

IN|FIDEM

Conférenciers

- Matthieu Chouinard
  Président & Fondateur
  In Fidem inc.
  matthieu.chouinard@infidem.biz
  www.infidem.biz

- Mathieu Roseau
  Responsable Développement Commercial
  Brainwave Canada
  mathieu.roseau@brainwaveidentitygrc.com
  www.brainwave.fr

Agenda

- Constats du marché
- Un marché émergeant : IAI
- Technologie et innovation IGRC
- Démonstration en direct
  - Cartographie dans les environnements Microsoft
  - Contrôle dans les ERP
  - Analyse dans le Cloud
  - Simplification des revues
  - Analyse comportementale des accès
- Cas client : CBC/Radio Canada

BRAINWAVE

BRAINWAVE & INFIDEM

Le marché, nos constats

Principales Fonctionnalités

IAI
Identity Analytics and Intelligence

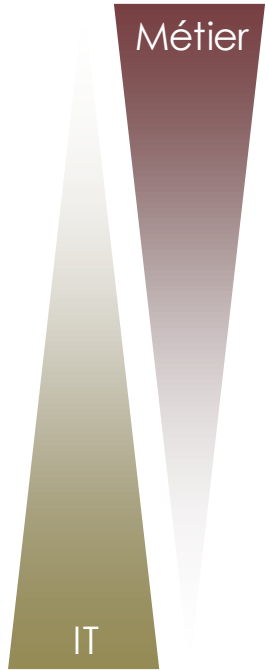
Pilotage, Contrôles, Audits, Analyses
- **Analyse** des habilitations et droits fins
- Plan de **contrôle** d'audit (y compris SoD)
- Suivi **historique** des changements
- **Reporting** et Tableaux de bord

IAG
Identity and Access Governance

Gestion de Rôles et Revues
- Workflows de revues des droits
- Workflows de demandes d'accès
- Modélisation de Rôles
- Provisionnement des droits

IAM
Identity and Access Management

Gestion des comptes et des mots de passe
- Workflows d'entrée / sortie
- Provisionnement des comptes
- Synchronisation d'annuaires
- Password reset (questions challenge)



BRAINWAVE

Forrester : Mai 2015

FOR SECURITY & RISK PROFESSIONALS

Wake-Up Call: Poorly Managed Access Rights Are A Breach Waiting To Happen

Employee Access Governance Is Critical

April 28, 2015 | Updated May 18, 2015

By **Merritt Maxim** with Stephanie Balaouras, Alexander Spiliotes

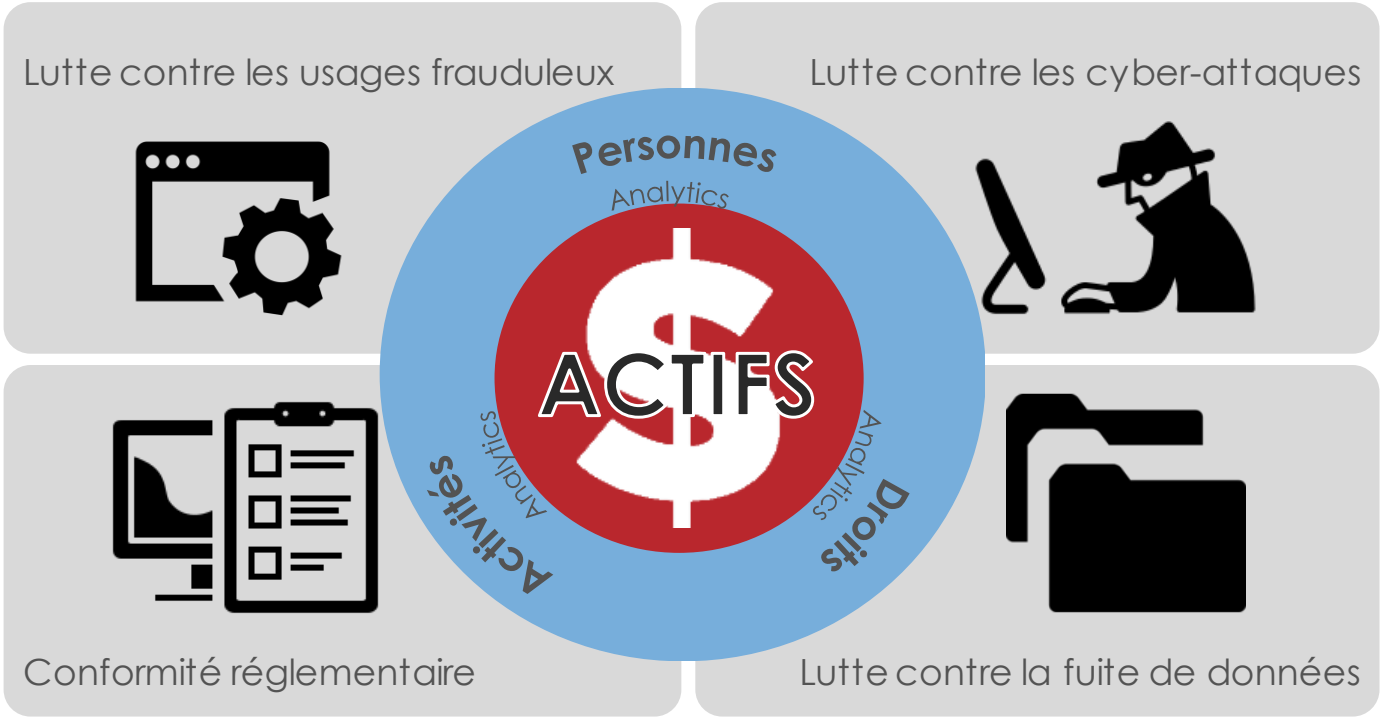
141 downloads

"Most security teams follow inconsistent procedures for conducting access reviews."

"Employees accumulate unnecessary access to sensitive data during their tenure . . . because of job changes, special projects and reorganizations."

BRAINWAVE

Valeur ajoutée de mieux contrôler la GIA



BRAINWAVE

BRAINWAVE & INFIDEM

Les défis auxquels vous faites face

1. Explosion du périmètre (nombre de systèmes, mobilité, infonuagique)

- 93% des entreprises utilisent des solutions en mode infonuagique
- 82% des entreprises ont une stratégie d'infonuagique hybride, soit une augmentation de 74% par rapport à 2014
- 88% des entreprises utilisant une solution en mode infonuagique utilisent ceux-ci en mode publique, contre 63 en mode privé

*Données provenant de l'étude de RightScale effectuée en janvier 2015 auprès de 930 professionnels des technologies de l'information

Gartner Prediction : The Death of "Least Privilege"

« By 2020, over 80% of enterprises will allow unrestricted access to non-critical assets reducing spending on IAM by 25%. »

2013 ISSA International Conference presentation: "The Gartner Identity and Access Management Scenario, 2014-2020."

BRAINWAVE

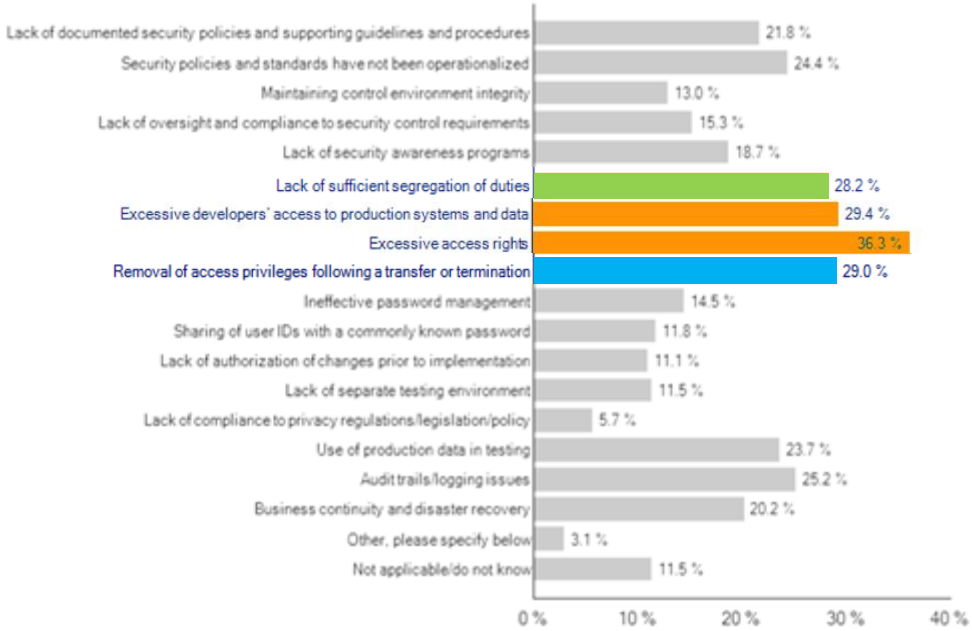
2. Incapacité d'avoir accès simplement à l'information sur les accès / permissions / droits accordés

- *M. Untel, à quels systèmes a t-il accès?*
- *Qui a quitté l'organisation dans les six derniers mois et a toujours des accès actifs sur nos systèmes ?*
- *Avez-vous désactivés tous les comptes des personnes qui ont quittés ?*
- *Les personnes qui ont changés de postes dans le dernier trimestre ont-elles encore accès aux anciens systèmes auxquels elles avaient droit?*
- *Qui peut accéder à :\\NAS\secret\verysecret\document.xls ?*
- *Y-a-t-il des utilisateurs pouvant se connecter à distance pour émettre des virements ?*
- *Est-ce que cette personne dans mon équipe est la seule qui a accès à ces données / systèmes ?*
- *Qui a revu ces accès la dernière fois ?*

BRAINWAVE

3. Enjeux de conformité sur la gestion des accès

Top 4 des écarts d'audits



Combinaisons toxiques de droits
Droits d'accès excessifs
Droits d'accès résiduels

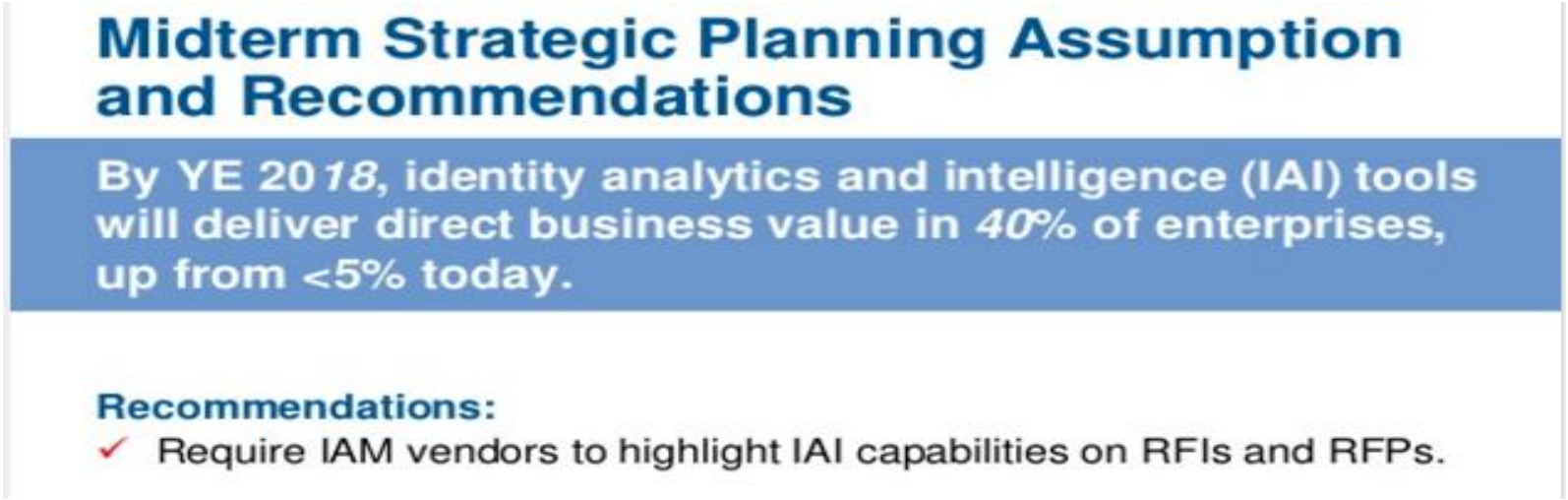
Deloitte, DTTL Global Financial Services Industry Security Study

IN|FIDEM BRAINWAVE

Gartner Prediction : Identity Intelligence Gets a Brain

« By year-end 2020, identity analytics and intelligence (IAI) tools will deliver direct business value beyond access and governance tools in 60% of enterprises. »

2013 ISSA International Conference presentation: "The Gartner Identity and Access Management Scenario, 2014-2020."



BRAINWAVE

Nos recommandations face à la GIA

- Optez pour une approche de déploiement rapide, à petit pas
  - Cartographiez, rationnalisez et nettoyez les référentiels
- Reprenez le contrôle sur vos informations en GIA : Misez sur le IAI
  - Exercez un contrôle des droits accordés aux utilisateurs
- Apportez de la valeur à vos métiers : Simplifiez leurs activités de revue des accès
  - Parlez leur langage, présentez l'information de façon à simplifier leurs tâches
- Démontrez votre conformité aux exigences face à la gestion des accès attribués aux utilisateurs (SOX, 52-109, PCI-DSS)
  - Mettez en place des contrôles en continu / automatisé

IN|FIDEM BRAINWAVE

BRAINWAVE & INFIDEM

Une approche structurée basée sur l'Analyse et l'Intelligence des Accès

Terminologie Gartner

IGA
Identity Governance and Administration

IAI
Identity Analytics and Intelligence

- Pilotage, Contrôles, Audits, Analyses

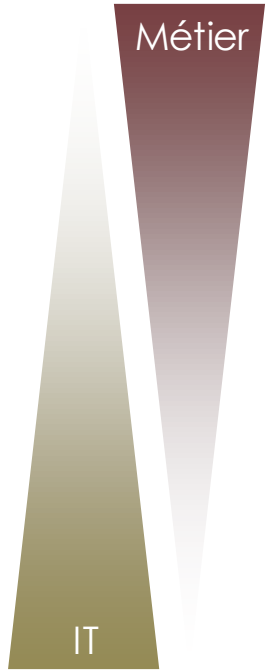
IAG
Identity and Access Governance

- Gestion de Rôles et Revues

IAM
Identity & Access Management

- Gestion des comptes et des mots de passe

BRAINWAVE



BRAINWAVE

Positionnement Brainwave en IAI

Gartner 2013 CoolVendor

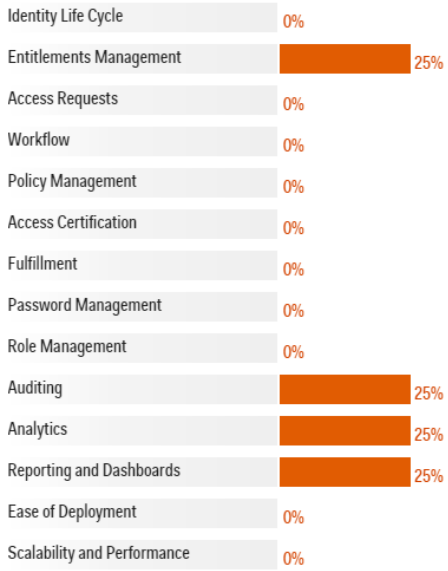
Gartner
A 2012 Niche Player
IAG Magic Quadrant

Identity Analytics & Intelligence

(as of Jan 2015)

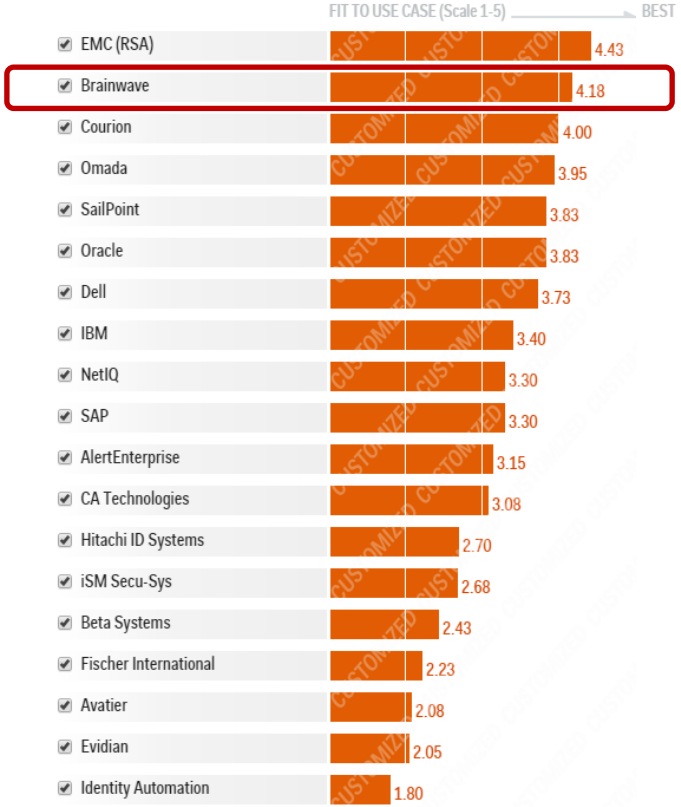
It encompasses a variety of technologies used for collecting, correlating, analyzing and reporting from identity, entitlement, activity and event data.

Capabilities and Weightings



Product Scores

Sort by score

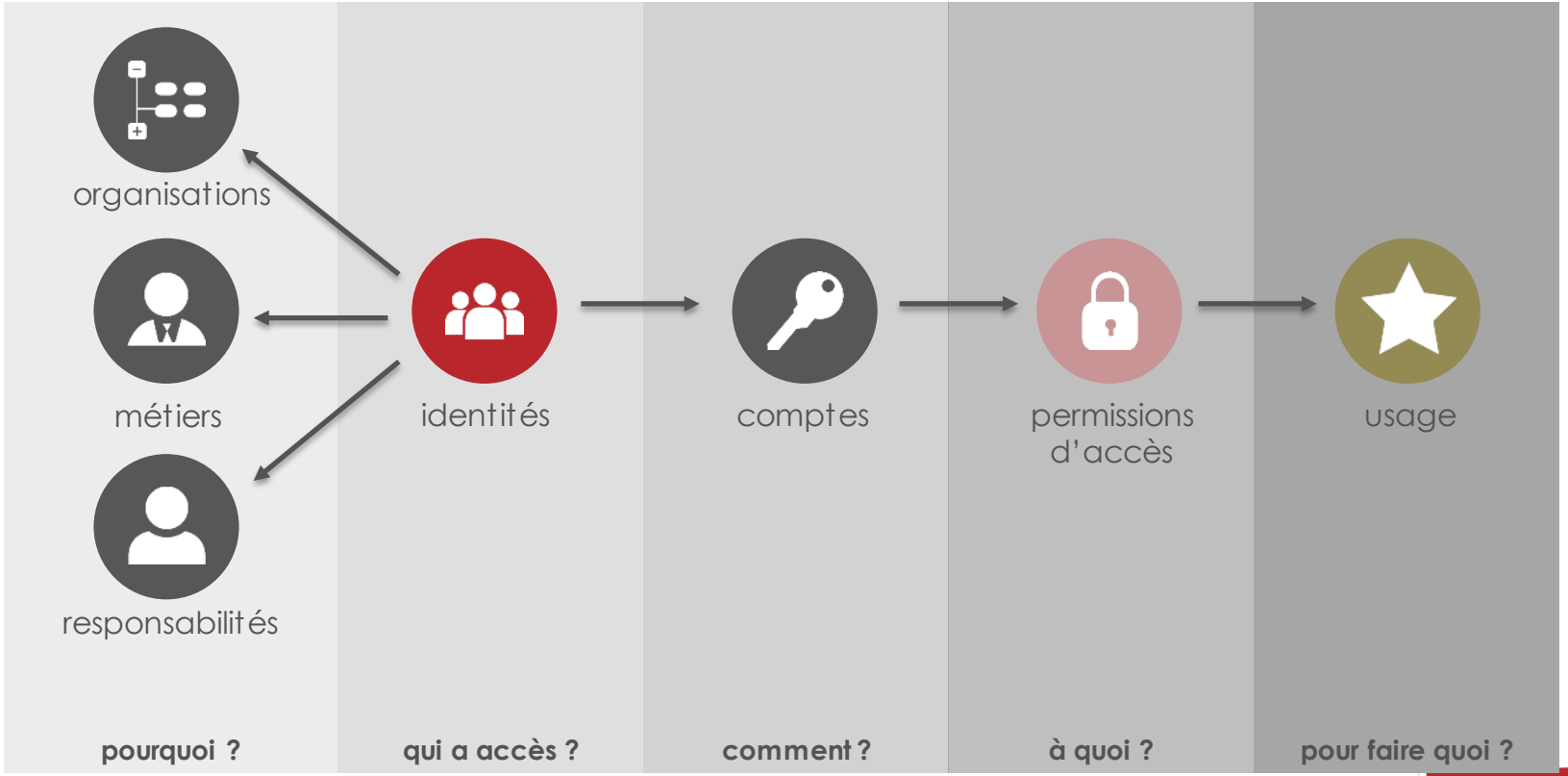


BRAINWAVE

BRAINWAVE & INFIDEM

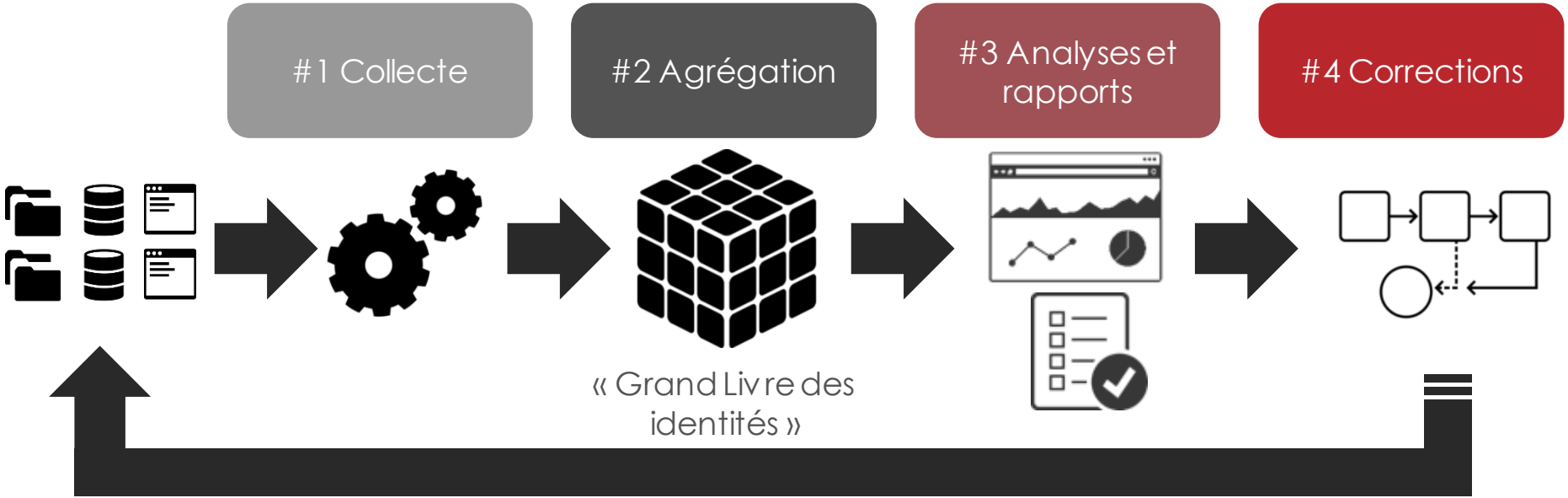
La technologie

Au cœur du Grand Livre des Identités



BRAINWAVE

Approche de contrôle continu avec Brainwave



BRAINWAVE

BRAINWAVE

Démonstrations

BRAINWAVE

Apporter rapidement de la visibilité sur l'environnement Microsoft

Fileshare, Sharepoint, Exchange

BRAINWAVE

Environnement Microsoft : qui fait quoi et comment?

?

Puis-je savoir rapidement et sans effort ce qu'il se passe dans mes environnements ?

SharePoint

Exchange

Office 365

Windows Server Active Directory

Windows Server

Microsoft SQL Server

Reprenez la main en un temps minime sur vos données !

BRAINWAVE

BRAINWAVE

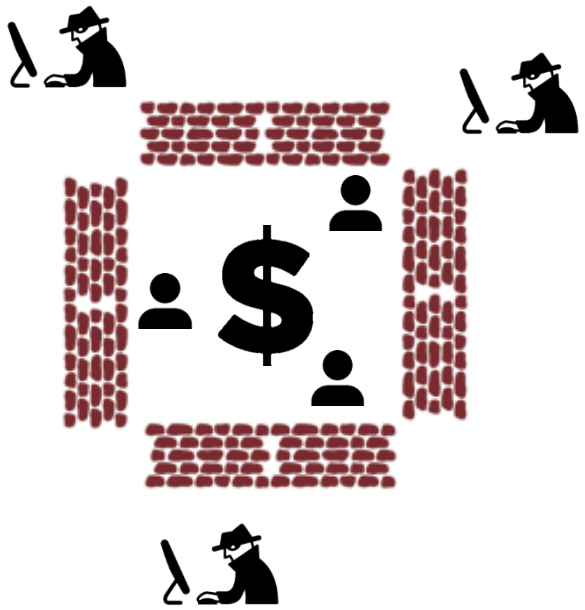
L’analyse des droits dans les nuages

CRM, Gdrive, …

BRAINWAVE

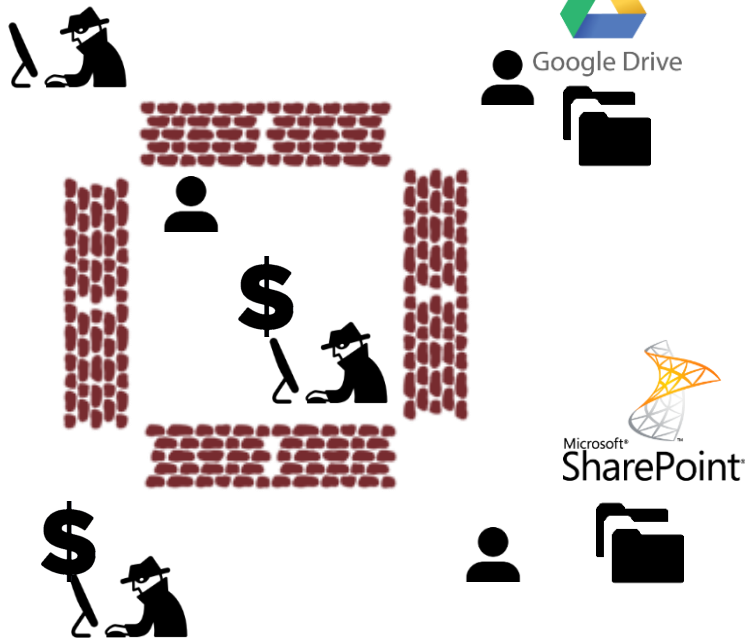
Transformation et contrôle des accès dans l'infonuagique

Sécurité périmétrique



Transformation digitale
Cloud, BYOD, shadow IT

???



Les données sont partout
Le focus doit être fait sur la donnée et les gens qui peuvent y accèder

BRAINWAVE

BRAINWAVE & INFIDEM

Effectuer des revues régulières : le challenge

A quoi ressemble la recertification pour les chargés de conformité

IN|FIDEM BRAINWAVE

Comment les responsables voient la recertification

« Merci de mettre vos initiales en bas de page et de signer sur la page 1389 »

IN|FIDEM BRAINWAVE

BRAINWAVE

Contrôler les transactions sensibles sur les ERP

SAP, Oracle Business Suite, Coda, …

BRAINWAVE

Pourquoi outiller le contrôle sur les ERP

Présence incontournable dans les activités

Réduire les risques de fraude

Répondre aux enjeux de conformité

Améliorer l'efficacité lors des audits

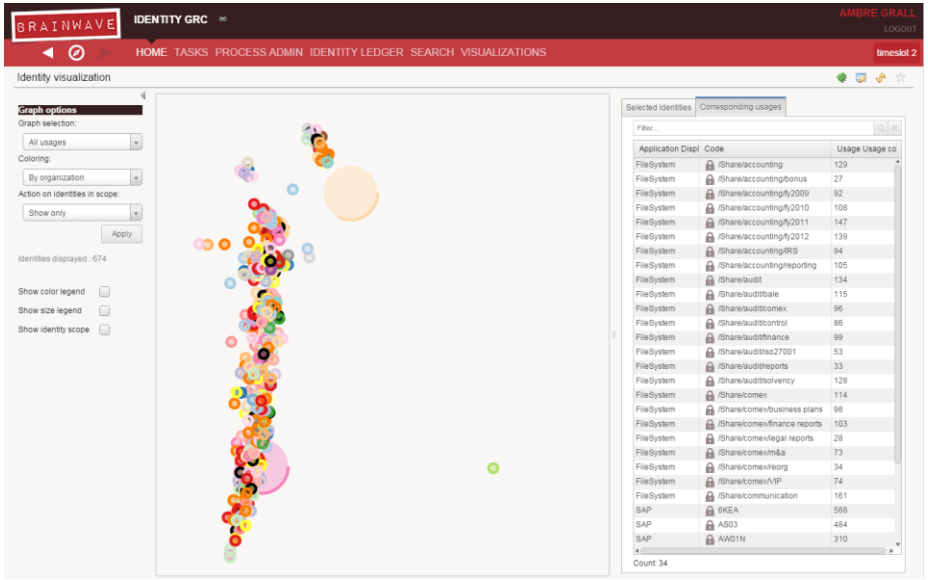
BRAINWAVE

BRAINWAVE & INFIDEM

L’intelligence de l’analyse : UBA

Brainwave User Behavior Analytics

- Analyse des logs d'accès
- Mise en évidence des situations anormales
  - Par rapport à des groupes de référence
  - Dans le temps
- Détection des signaux faibles
  - Vol de données
  - Collusion
  - Fraude
  - Comptes compromis
- A destination des analystes sécurité
  - Analyse à forte valeur ajoutée des données du SIEM



BRAINWAVE

Brainwave UBA

Pourquoi est-ce unique sur le marché?

Algorithmes dédiés de modélisation comportementale et d'analyse graphique

Capitalisation sur la notion de « Timeslot » pour réaliser le baselining

Capitalisation sur le « business context » pour identifier les groupes de référence

BRAINWAVE

Cas d'application

Monitoring des données et des transactions sensibles

- Vol de sensibles sur les partages disques sensibles (RH, Finance)
  - Accès par un « curieux »
  - Récupération des données avant un départ d'un collaborateur…
- Collusion sur l'ERP

  Comptable A émet des factures + Comptable B règles les factures
  - Identification de comportements anormaux dans la même échelle de temps
- Rogue admin
  - Un administrateur technique a un usage anormal du PAM (trop de demandes, demandes en dehors des périodes habituelles, demandes sans trace dans l'outil de ticketing associé…)

BRAINWAVE

BRAINWAVE & INFIDEM

Le produit

Principales Fonctionnalités

Recherches et Investigations

Recherches en langage naturel, navigation à 360°

Revues

Revue des identités, comptes, droits
Gestion de processus (revues partielles, des problèmes, suivi des corrections…)

Tableaux de Bord

Métriques de pilotage, changements et problèmes

Reporting

Publication et export (Excel, Word, PDF), envoi par mail

Moteur de règles

Requêtes multi-dimensionnelles sur de grands volumes de données

Plan de Contrôle

Contrôle des droits fins, Combinaisons toxiques, Droits théoriques

Moteur d'Analyses

Aide à la décision, droits standard (mining), analyse comportementale

Grand Livre des Identités

Catalogue des permissions et historique des données : identités, comptes, permissions, usages
Propriétaires de comptes, groupes, applications, permissions… Suivi des exceptions et dérogations

Découverte de données

Analyse et préparation des données pour le chargement

Moteur de collecte

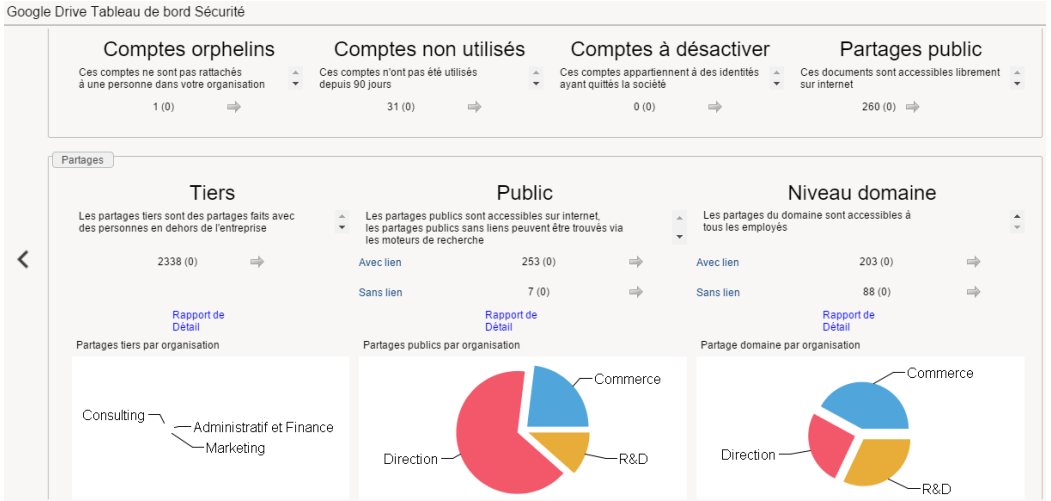
Nombreuses applications préconfigurées à télécharger

Cas client
Radio Canada

Radio Canada

Objectif

- Identifier les risques sur les partages de documents sous Google Drive
- Assurer les revues en ligne au travers du Workflow et du portail
- Automatiser et assurer l'exhaustivité des contrôles
- Améliorer la visibilité sur les mouvements de personnes et sur l 'évolution de leurs droits
- Mettre en œuvre les contrôles SoD



Mission

- Construction d'une vision centralisée des utilisateurs et de leurs autorisations
- Import de règles de SoD pour préparer les campagnes d'audit
- Confrontation des résultats avec les gestionnaires impliqués et définition de plans d'actions

Contrôler les habilitations

Éléments clés

- ~ 9500 utilisateurs
- Implémentation d'une dizaine d'applications (comprenant Google Drive et SAP)
- Automatisation des contrôles
- 40 jours d'implémentation

Une approche complémentaire avec la GIA

ACT

PLAN

DO

CHECK

REDUCTION DES RISQUES

EFFICACITE OPERATIONNELLE

Solution GIA

- Cycle de vie des habilitations
- Arrivées/départs/mouvements

Processus de gestion

- Demandes
- Validations
- Gestion des comptes d'accès
- Gestion des droits

- (Automatisation des actes techniques)
- Controles de séparation de taches au niveau rôle (sur droits théoriques)

Solution Brainwave

- Cartographie des utilisateurs et de leurs droits réels sur les systèmes
- Mise en évidence des incohérences
- Automatisation des contrôles sur les données réelles
  - Principes de moindre privilège
  - Séparation des taches
- Préparation des revues de compte
- Consolidation d'indicateurs sur les écarts et les risques associés

Pourquoi Brainwave est-il unique ?

Approche Security Intelligence
Corrélation des personnes, des droits et des comportements

Analyse et contrôle en continu
Changements, dérives, écarts et incohérences

Hautement personnalisable
Intégration aisée des applications internes, moteur de workflow avec éditeur graphique

Tous types d'actifs
Systèmes, applications, cloud, ressources physiques…

Actionnable
Tableaux de bord de pilotage, suivi et remédiation des risques, gouvernance

Performant
Analysez des millions de droits d'accès en quelques secondes

BRAINWAVE

Merci et n’hésitez pas à venir nous discuter avec nous !

BRAINWAVE

BRAINWAVE & INFIDEM

Les Sociétés

Les sociétés In Fidem et Brainwave

IN|FIDEM

- Experts-conseil en sécurité de l'information
- A deux Centres d'expertise spécialisés en GRC et en GIA
- Partenaire Platinum Brainwave depuis 2014

BRAINWAVE

- Éditeur Français de solutions de sécurité informatique
- Au Québec depuis 2014.
- Clients présents dans 9 pays
- De nombreuses récompenses du marché (Cool Vendor Gartner, Carré Magique GIA Gartner, etc…)

IN|FIDEM BRAINWAVE

Brainwave - Historique

Clients dans 9 pays
Bureaux en Europe et au Canada

HEXATRUST
CYBERSECURITY & DIGITAL TRUST
membre fondateur

2015

3 fondateurs

2010

prix de l'innovation des assises 2011

2011

Gartner
A 2012 Niche Player
IAG Magic Quadrant

2012

Gartner 2013
CoolVendor

2013

Trophée innovation IT 2014

LeadershipCompass KuppingerCole

2014

Quelques clients