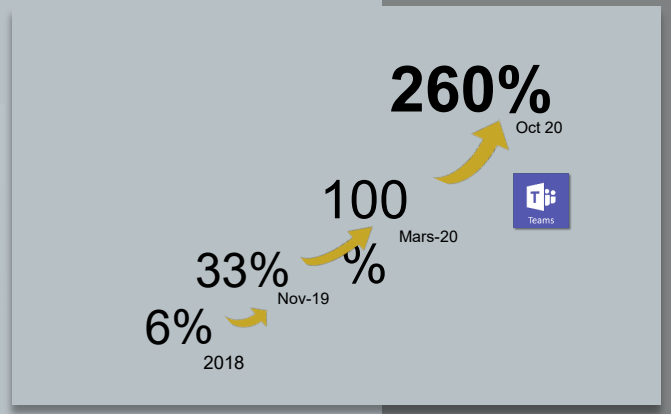
PLACE DES UTILISATEURS FINAUX DANS LA SÉCURITÉ D'OFFICE 365

DANIEL REZLAN - IDECSI

Julie et toute son équipe utilisent Office 365

Elle peut facilement partager ses Teams, ses dossiers OneDrive, SharePoint, donner des accès, consulter ses fichiers, ses mails de l'extérieur, connecter ses devices…



Pierre, les équipes sécurité, workplace et IT sont inquiets

Comment sécuriser les espaces collaboratifs, l'accès aux dossiers sensibles, suivre les partages, savoir qui accède à quoi, identifier une compromission, un accès malveillants…et les hackers

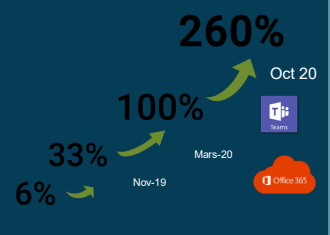
2020

RSA

FIC

Thème central : HUMAN ELEMENT

FIL ROUGE "Replacer l'humain au cœur de la cybersécurité"



sondage JDN / Club Décision DSI auprès de sociétés basées en France

Microsoft data

Accélération utilisation Teams et outils Collaboratif
= forte augmentation accès, partages...

45%

Des collaborateurs sont inquiets

25%

N'utilisent pas les outils de l'entreprise par crainte pour leurs données

Étude pour Idecsi – Nov 19
"Les salariés et la sécurité des données"

81%

Des utilisateurs souhaitent pouvoir consulter qui accède, qui a des droits sur leurs ressources

Étude pour Idecsi – Nov 19
"Les salariés et la sécurité des données"

CONTEXTE

Parmi les enjeux sécurité 2 grands objectifs

Maîtriser le cycle de vie de la donnée

S'assurer que les données, les Teams, sont accédés et partagés par et avec les bonnes personnes

Corriger les erreurs de configuration

Contrer une fraude

Identifier une compromission le plus vite possible

N°1

Baromètre CESIN-Opinionway 2020

Top enjeu cyber
Hygiène des droits - Qui fait quoi ?

OBJECTIFS ET ENJEUX

IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

1

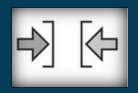
Ce qu'il faut être en mesure de savoir et de faire

2

Ce que cela nécessite

Difficultés

Facteurs de contraintes



3

Facilitateurs

Facteurs favorables

4

1

ÊTRE EN MESURE DE

Savoir qui fait quoi, partage quoi ? Avec qui ? Qui a fait quoi ? accède à quoi ?...

Détecter si un accès, un partage, une configuration sont illégitimes ou malveillants

-> utilisateurs, admin, device, application et erreur humaine

Corriger et remédier, aussi vite que possible, les problèmes identifiés

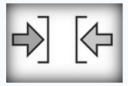
Maîtriser et maintenir la justesse des droits et des partages dans le temps

2

Ce que cela nécessite

Difficultés

Facteurs de contraintes



3

Facilitateurs

Facteurs favorables

4

IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

1

Ce qu'il faut être en mesure de savoir et de faire

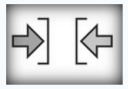
2

CE QUE CELA NÉCESSITE - BESOIN DE :

Monitorer l'ensemble des accès, droits et des configurations
Disposer d'un outil d'analyse et d'audit
Distinguer les événements légitimes des événements malveillants : activité normale vs problèmes
-> avoir un process de lever de doute rapide et simple
-> Monitoring personnalisé pour chaque user et ressource : éviter nb d'alertes trop important
Identifier quelles sont les mises à jour nécessaires : retrait de droits, arrêt partage...

Difficultés

Facteurs de contraintes



3

Facilitateurs

Facteurs favorables

4

IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

1

Ce qu'il faut être en mesure de savoir et de faire

2

Ce que cela nécessite

DIFFICULTÉS / COMPEXITÉ

Grand Volume : users x applications x partages x accès
Évolution permanente et changements nombreux dans le temps
Difficulté pour un user de voir ce qui se passe sur ses données et de corriger

Facilitateurs

Facteurs favorables

3

4

IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

1

Ce qu'il faut être en mesure de savoir et de faire

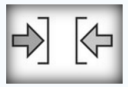
2

Ce que cela nécessite

3

Difficultés

Facteurs de contraintes



4

FACILITATEURS - FACTEURS FAVORABLES

Awareness sécurité des utilisateurs
Adoption des bonnes pratiques hygiène sécurité : gestion des droits sur ses données
Autonomie équipes sécurité / workplace sur le suivi

IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

1

ÊTRE EN MESURE DE

Savoir qui fait quoi, accède à quoi, comment, depuis où, partage quoi, avec qui ?...

Qui a des droits sur qui, sur quelles ressources ?

Savoir qui a fait quoi... ? -> Tracer, investiguer, forensic

Détecter si un accès, un partage, une configuration sont illégitimes ou malveillants

-> fait par un utilisateur, un administrateur, un appareil, une application

Identifier les erreurs humaines

Corriger et remédier, aussi vite que possible, les problèmes identifiés

2

CE QUE CELA NÉCESSITE - BESOIN DE :

Monitorer l'ensemble du tenant sur les accès, les objets de configuration

Disposer d'un outil d'analyse et d'audit ergonomique – clarté restitution

Monitoring personnalisé pour chaque user et ressource : éviter nombre d'alertes trop important

Distinguer les événements légitimes des événements malveillants – activité normale vs problèmes

-> avoir un process de lever de doute rapide et simple

Identifier les mises à jour nécessaires

DIFFICULTÉS

Grand Volume : users x applications x partages x accès

Difficulté pour un user de voir ce qui se passe sur ses données et de corriger

Évolution permanente dans le temps

Complexité

3

FACILITATEURS – FACTEURS FAVORABLES

Awareness sécurité des utilisateurs

Confiance utilisateurs

Adoption des bonnes pratiques hygiène sécurité : gestion des droits sur ses données

Autonomie équipe sécurité / workplace sur le suivi

4

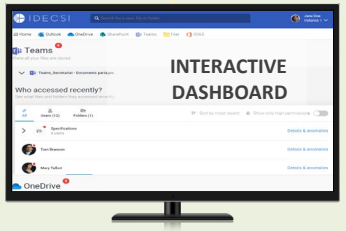
IMPLIQUER LES UTILISATEURS DANS LA MAÎTRISE DU CYCLE DE VIE DE LA DONNÉE – DÉTECTION DE FRAUDE

UN PROCESS AUTOMATISÉ ET SOUS CONTRÔLE

ACCÈS
PARTAGES
DROITS
CONFIGURATIONS

SharePoint
Teams
OneDrive

1
Permet visibilité et capacité d'analyse



Individuel
Centralisé
A jour en permanence
Disponible à la demande
Envoyé lors de campagnes
Envoyé à fréquence régulière

NOTIFICATIONS

En temps réel

2
Identification temps réel des uses case de fraudes avérées

3
Adoption + users gestion simplifiée et en un seul point

Identification rapide

4
Augmente et maintient awerness sécurité et confiance utilisateurs

5
Augmente considérablement capacité et fiabilité de détection

Accès malveillants, droits obsolètes

CORRECTION REMEDIATION DIRECTES

Arrêt malveillances

Retrait droits, partages obsolètes, erreurs humaines...

Opérations, accès changements légitimes

VALIDATION

Mise à jour des accès, devices, droits légitimes,

6
Réduit effort de remédiation

8
Forte réduction des vulnérabilités liées aux configurations / Partages / droits

MONITORING DES EQUIPES SECURITE

SOC - SIEM
CISO TEAM

RECERTIFICATION
A FREQUENCES REGULIERES

O365 SAIN ET A JOUR

9
Maîtrise dans le temps des configurations / Partages / droits