La cybersécu un enjeu (encore plus) prioritaire pour les organisations

Projetlys

Mardi 5 avril 2022

blue soft GROUP

Les intervenant·es

Guillaume Petit
Ingénieur d'affaires

Jean-François Bérenguer
Directeur des Opérations

Blandine Pinto
Consultante Avant-Vente
Adoption Office 365

Agenda

01. Contexte

02. Comment renforcer rapidement et efficacement son SI ?

03. Sensibilisation des utilisateurs

04. La sécurité chez Projetlys

01. Contexte

Définitions

« La cybersécurité est un état recherché pour un système d'information lui permettant de résister à des événements issue d'internet et susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises »

Source ANSSI

« La cybersécurité est la protection des systèmes connectés à Internet contre les menaces informatiques visant le matériel, les logiciels et les données. »

Source Tech Target

Nouveau paradigme

La sécurisation des systèmes d'information est une guerre incessante qui **nécessite de se préparer aux attaques**.

La sécurité consiste a **comprendre les menaces** et à faire le nécessaire pour **les atténuer**, mais il est impossible de parer toutes les attaques.

C'est pourquoi, il est important **d'adopter une stratégie** et une **approche de défense** en profondeur fondées sur le risque.

Naviguer dans un monde en mutation

Les attaques se multiplient plus sophistiquées

Outils de sécurité conventionnels n'ont pas suivi le rythme

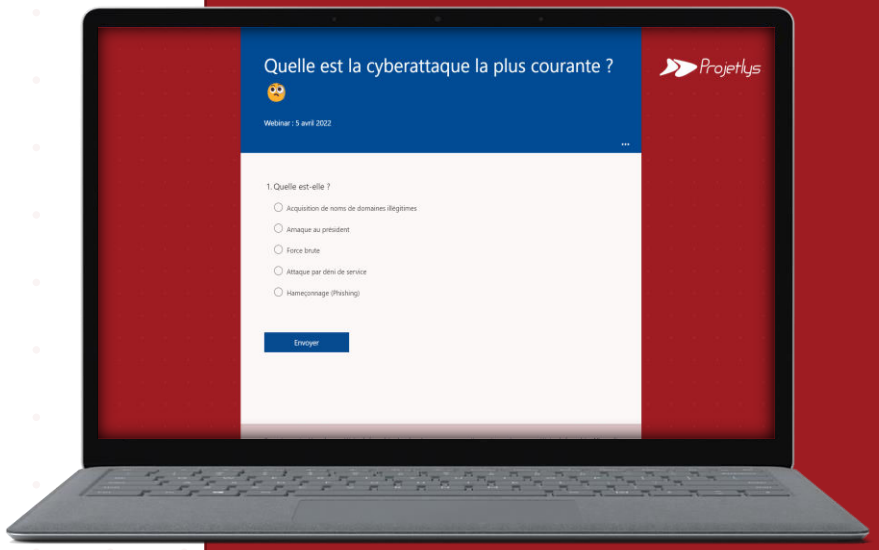
Paysage réglementaire devenant plus complexe

https://forms.office.com/r/uSbea4aJKB

SONDAGE

QUELLE EST LA CYBERATTAQUE LA PLUS COURANTE ?

Une petite idée ?

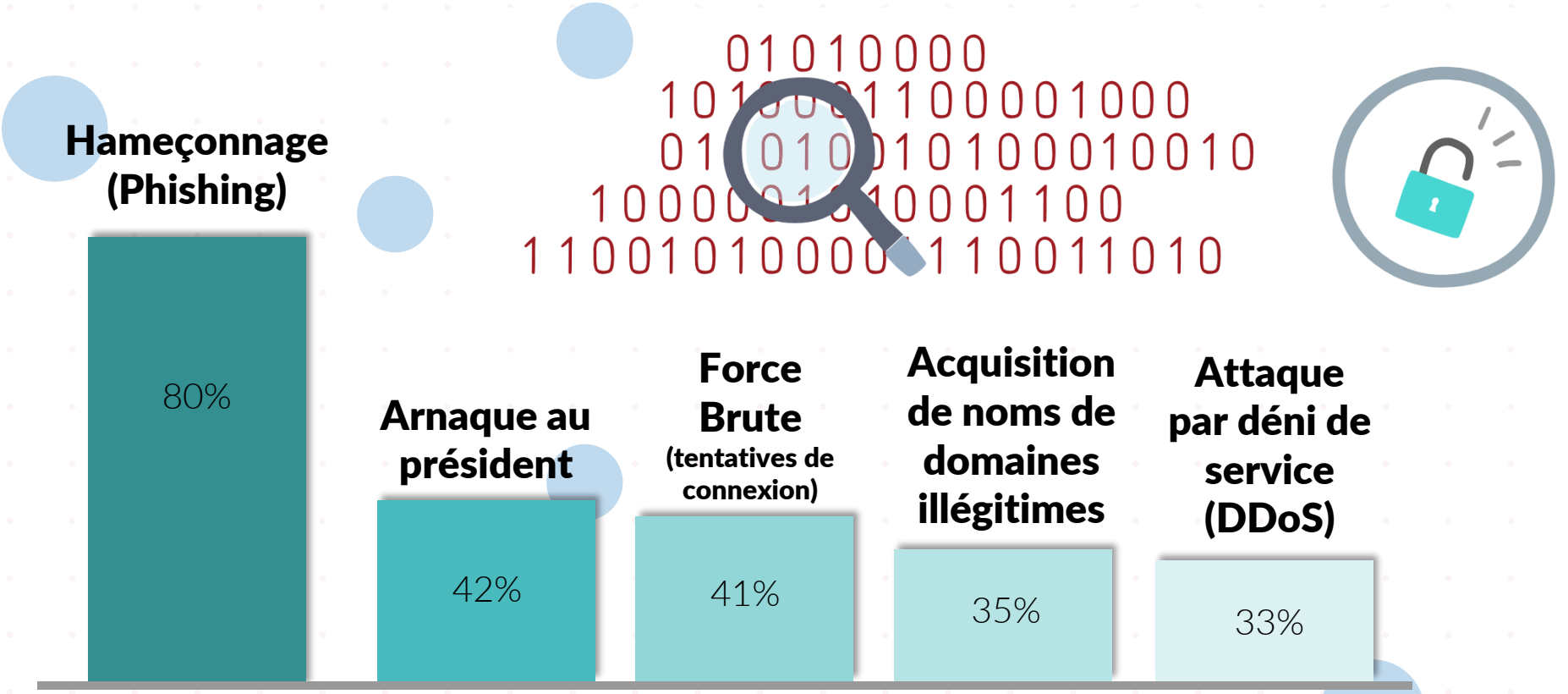


Projetlys

Projetlys

Les cyberattaques

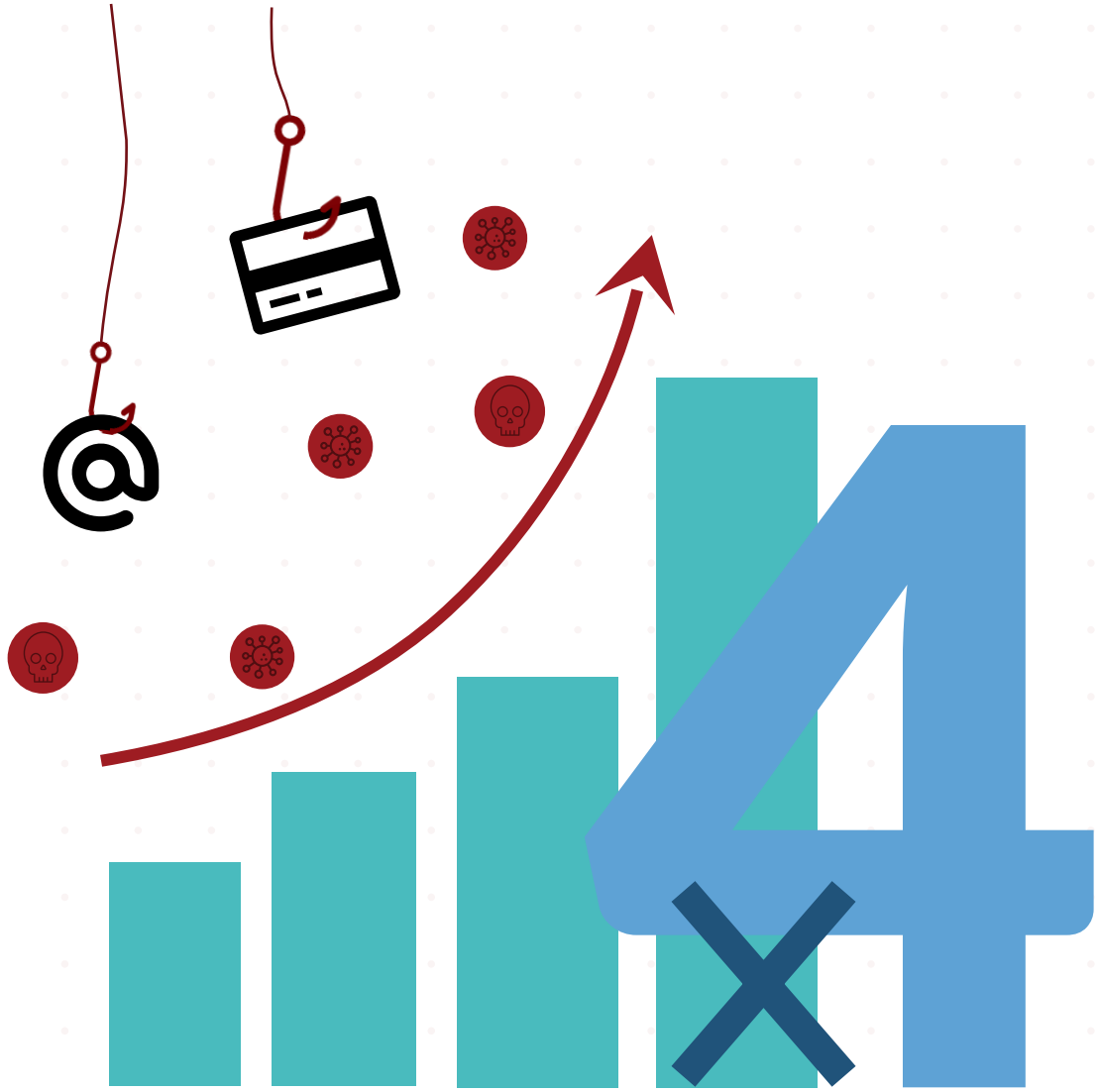
Les plus courantes contre les entreprises en 2020



Plusieurs réponses possibles. Sélection des plus fréquentes.

(source: statista)

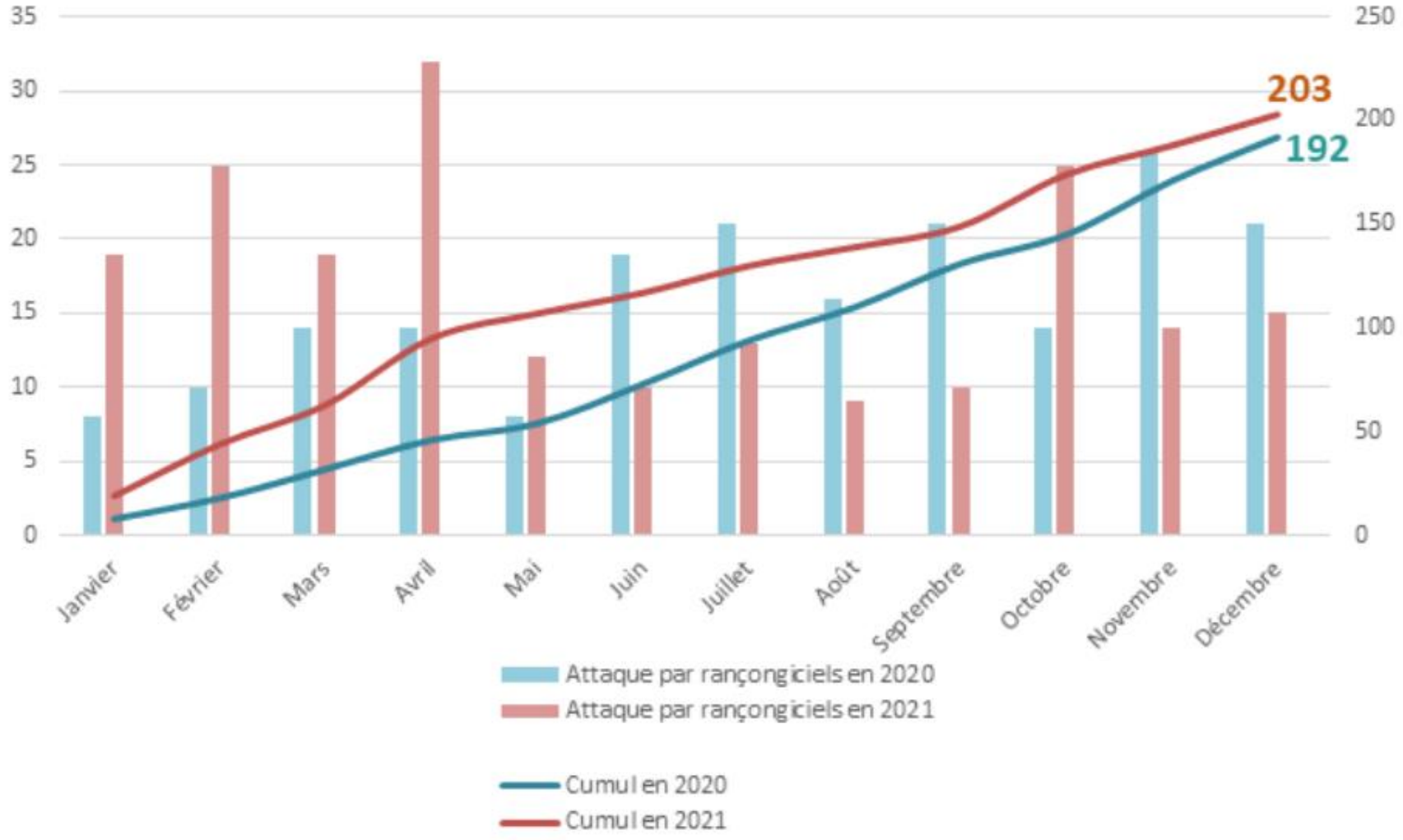
Force est de constater...



En 2020, le nombre de signalements liés à des rançongiciels a été multiplié par quatre par rapport à l'année 2019, d'après l'ANSSI

Agence nationale de la sécurité des systèmes d'information

Le rançonware encore en augmentation



Quelques chiffres

91%

Des organisations françaises ont été la cible **d'au moins une cyberattaque** au cours de 2020
(source: Proofpoint)

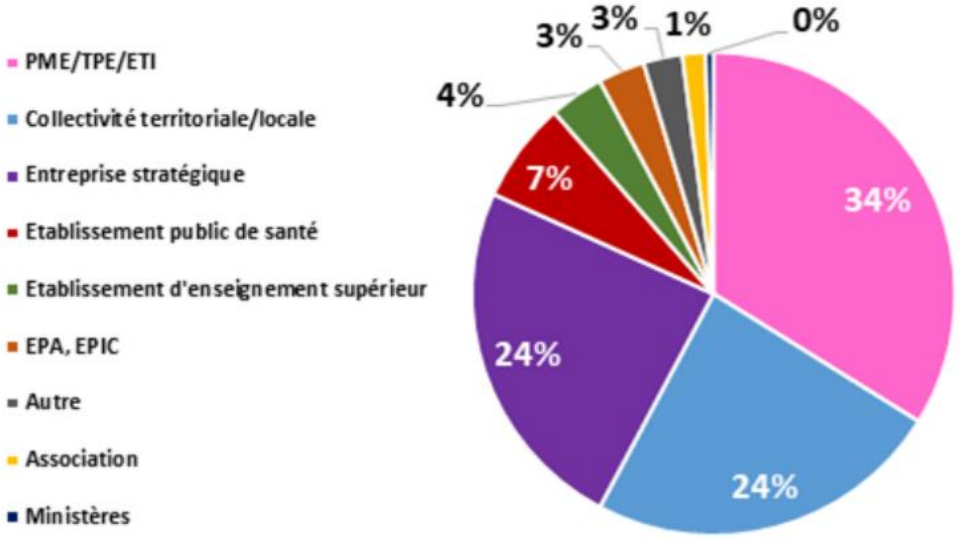
20%

jugent que les utilisateurs finaux ne sont pas équipés ou formés pour le télétravail
(source: Proofpoint)

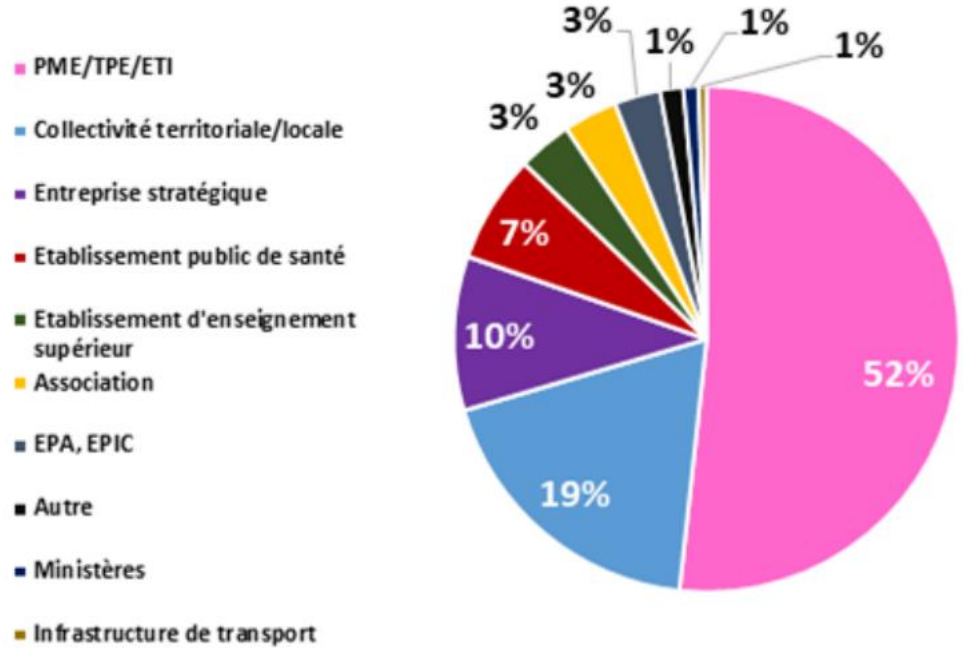
80%

des cyberattaques viennent de la gestion des identités

Répartition des entités victimes par rançonware



2020



2021

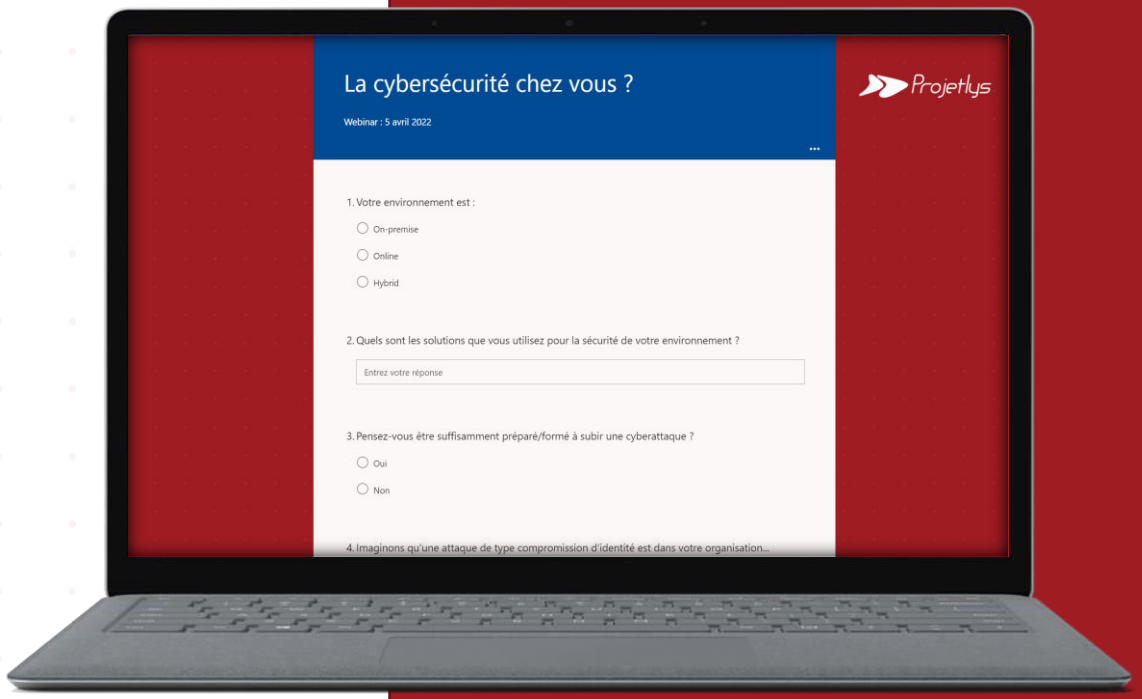
02. Comment renforcer rapidement et efficacement son SI ?

Projetlys

https://forms.office.com/r/86pUb4tqVt

SONDAGE

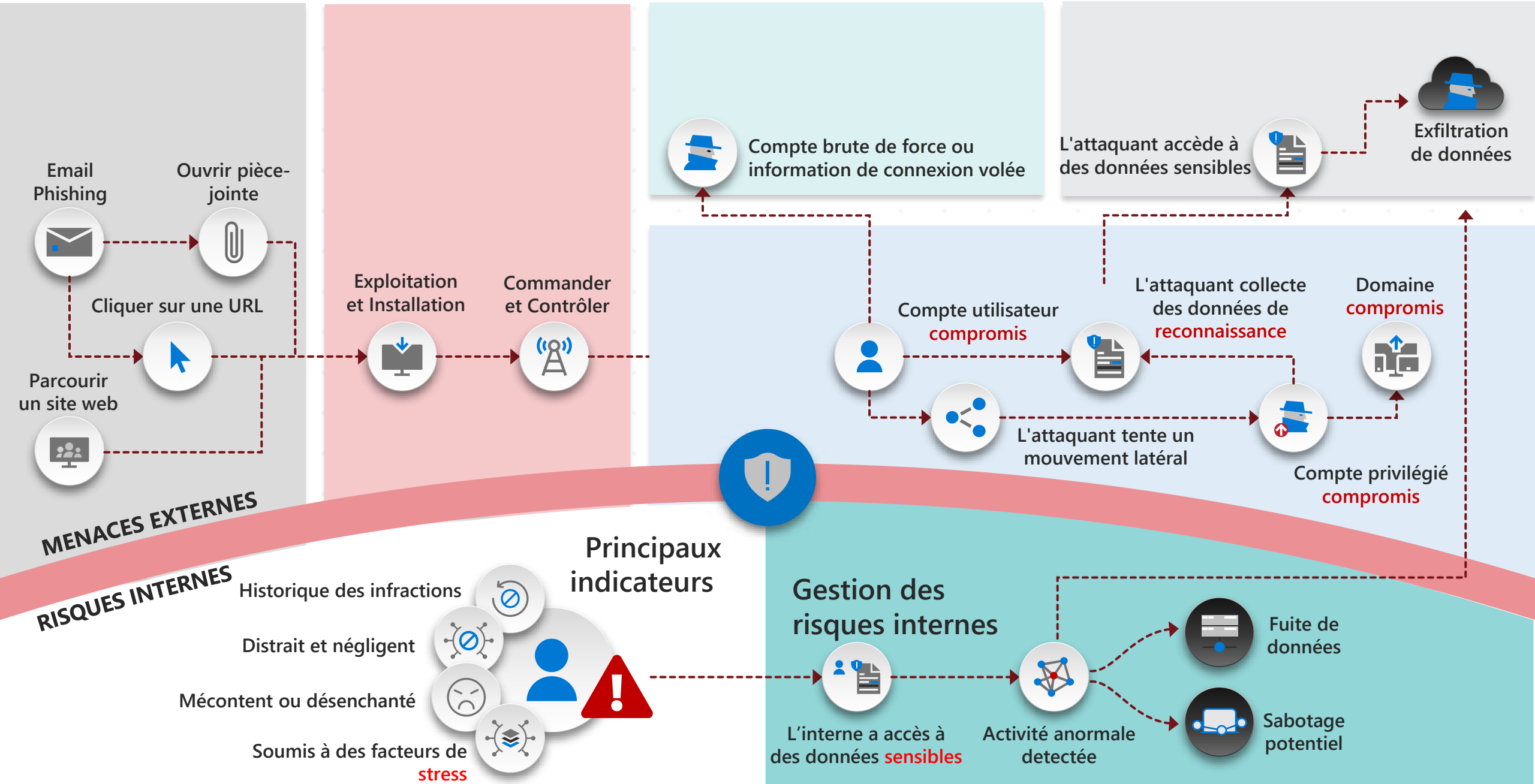
LA CYBERSÉCURITÉ CHEZ VOUS ?



Projetlys

Projetlys

Protection complète tout au long de la kill chain



Microsoft Zero Trust solution

Vérifier explicitement I Moindre privilège I Accepter la brèche

Utilisateur

- Groupes/Rôle
- Localisation
- Privilèges
- Session à risque
- Risque utilisateur

Périphérique

- Géré ou BYOD
- Santé et conformité
- Risque lié aux périphériques
- Type et version OS
- Chiffrement

Microsoft Azure AD

Defender for Identity

Defender for Endpoint

Microsoft Intune

Politique de sécurité et de conformité

Microsoft Information Protection

Microsoft Cloud App Security

Microsoft Cloud

Cloud SaaS apps

On-premises & web apps

Visibilité I Analyse I Automatisation

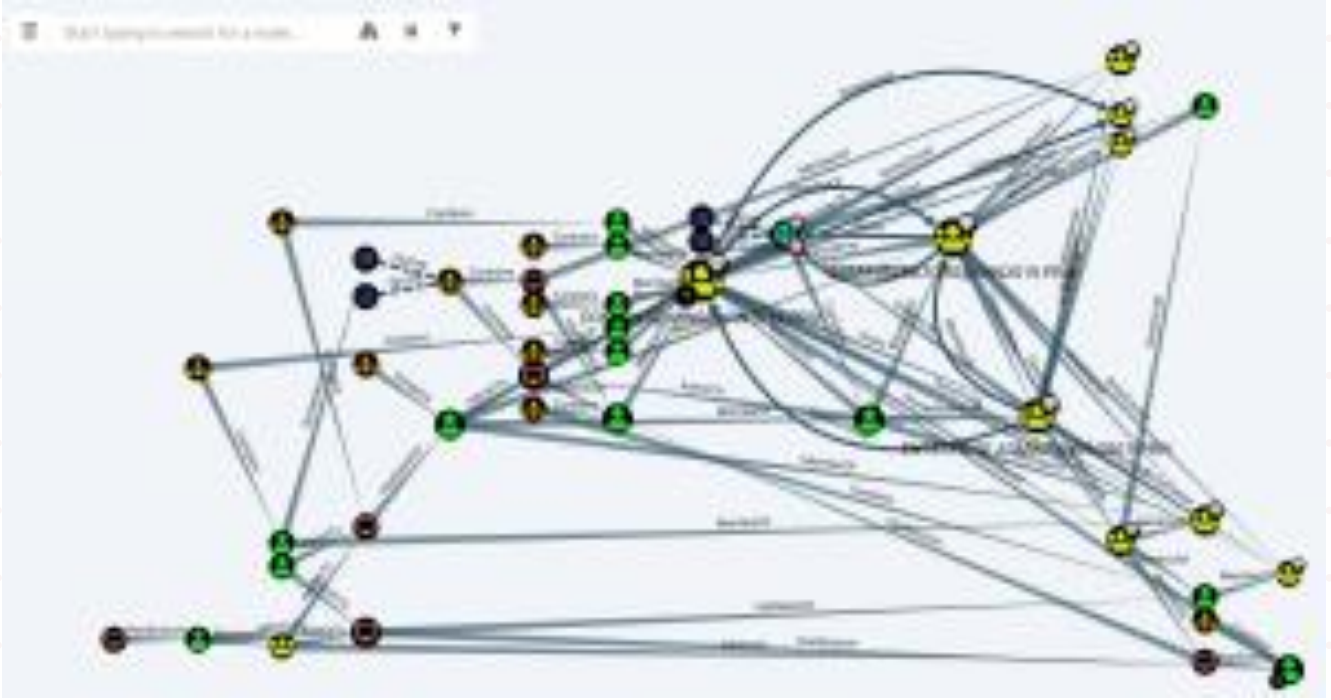
Azure Sentinel

Le mouvement latéral : définition

Parce que l'Active Directory est le maillon faible de la sécurité du SI

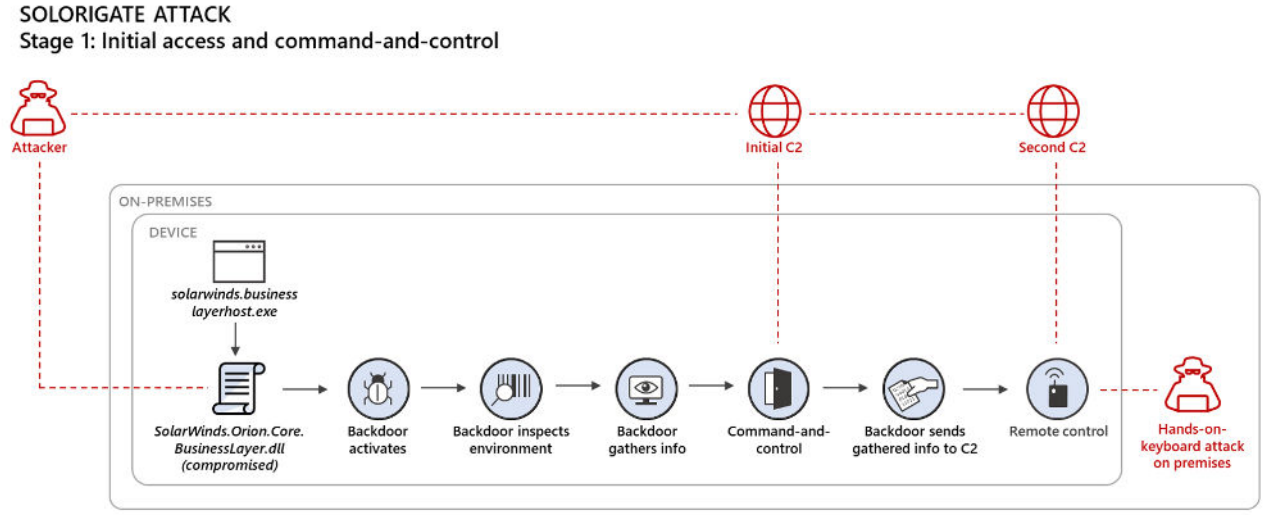
Utiliser des comptes non sensibles pour obtenir l'accès à des comptes sensibles dans votre réseau.

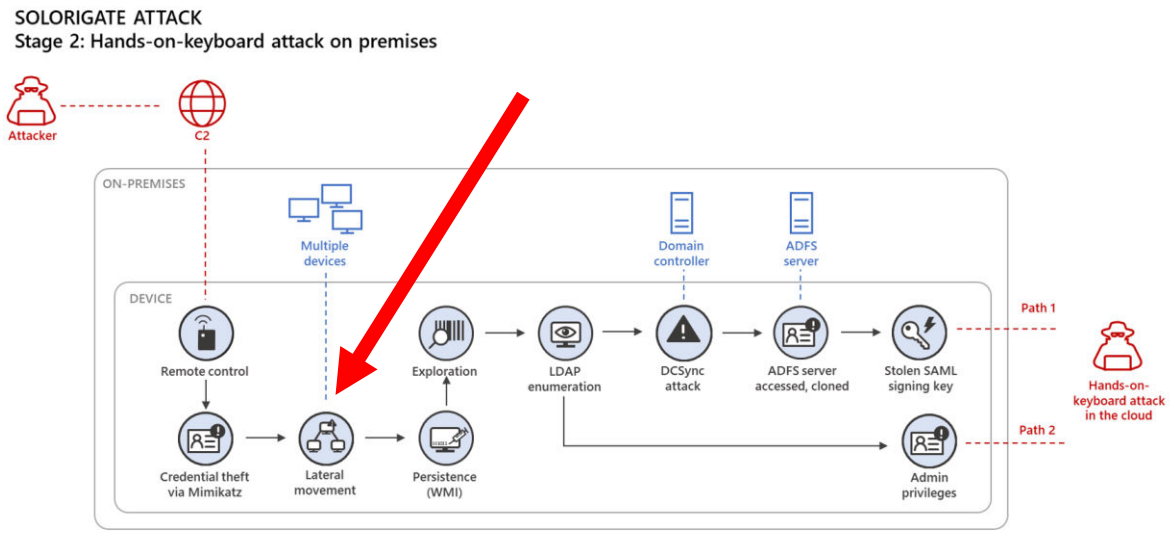
Exemple de cartographie avec BloodHound



Cybersécurité : Techniques de cartographie Active Directory avec BloodHound · iTPro.fr

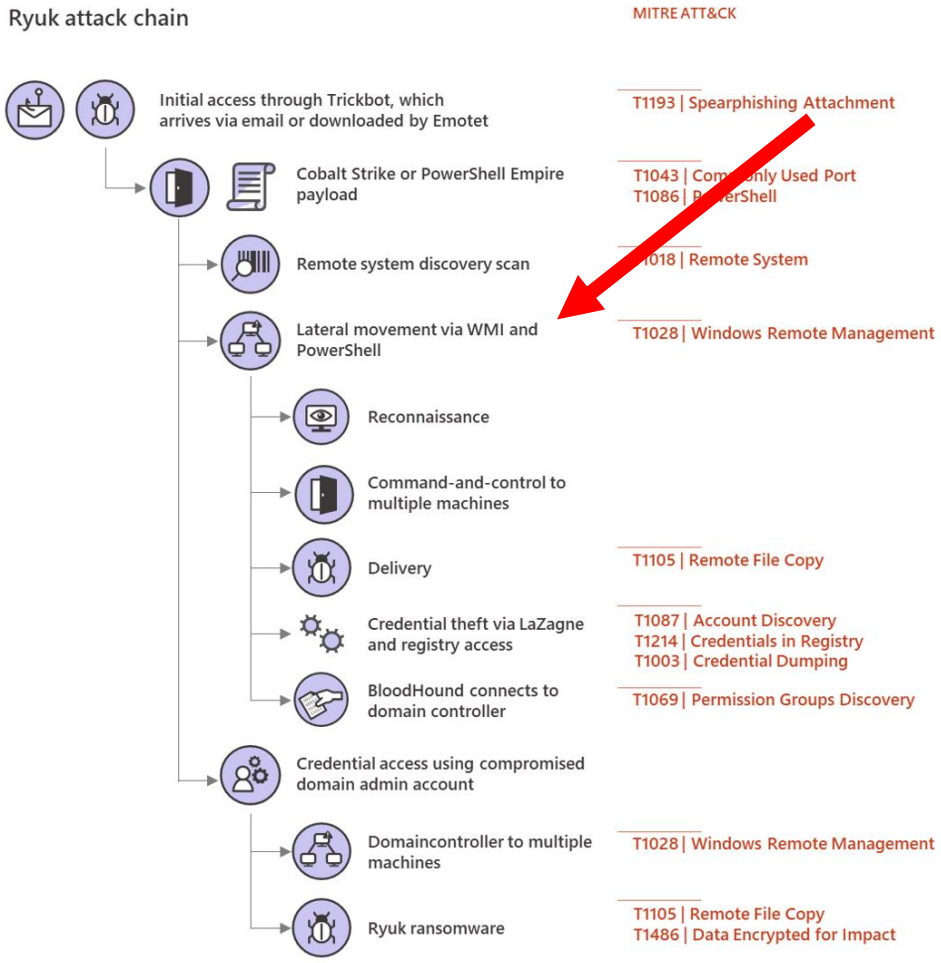
Très souvent utilisé

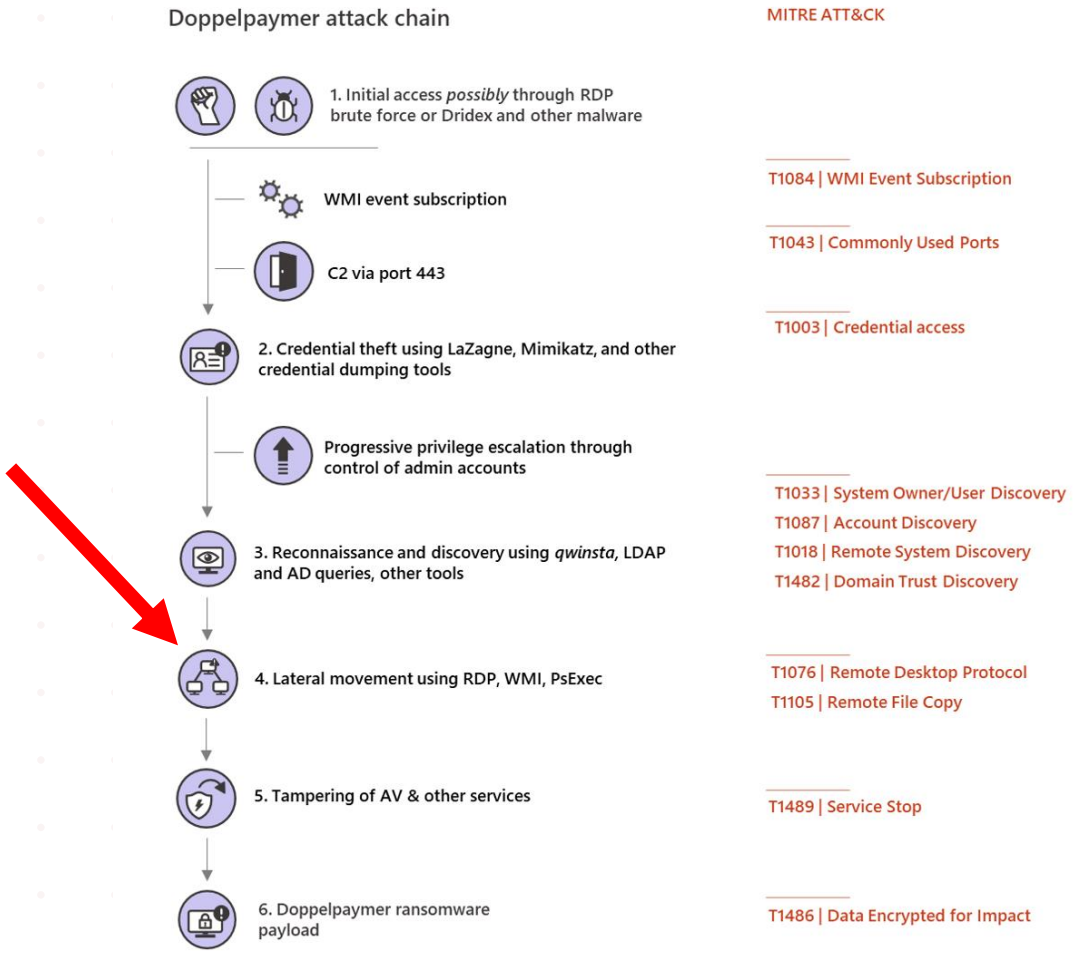




Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security Blog

Très souvent utilisé





https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Les bonnes pratiques : une question de bon sens

- Isolation des comptes
- Appliquer le principe du moindre privilège (moins de 5 admins globaux), et faire des revues régulières des comptes à privilèges
- Pas de connexion en tant qu'admin sur les postes utilisateurs
- Ecrire les règles de sécurité, les diffuser et contrôler leur conformité
- Mettre en place les moyens humains et les processus

Les bonnes pratiques (suite)

- Renforcer l'authentification sur les systèmes d'information
- Accroître la supervision de sécurité
- Sauvegarder hors-ligne les données et les applications critiques
- Établir une liste priorisée des services numériques critiques de l'entité
- S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque

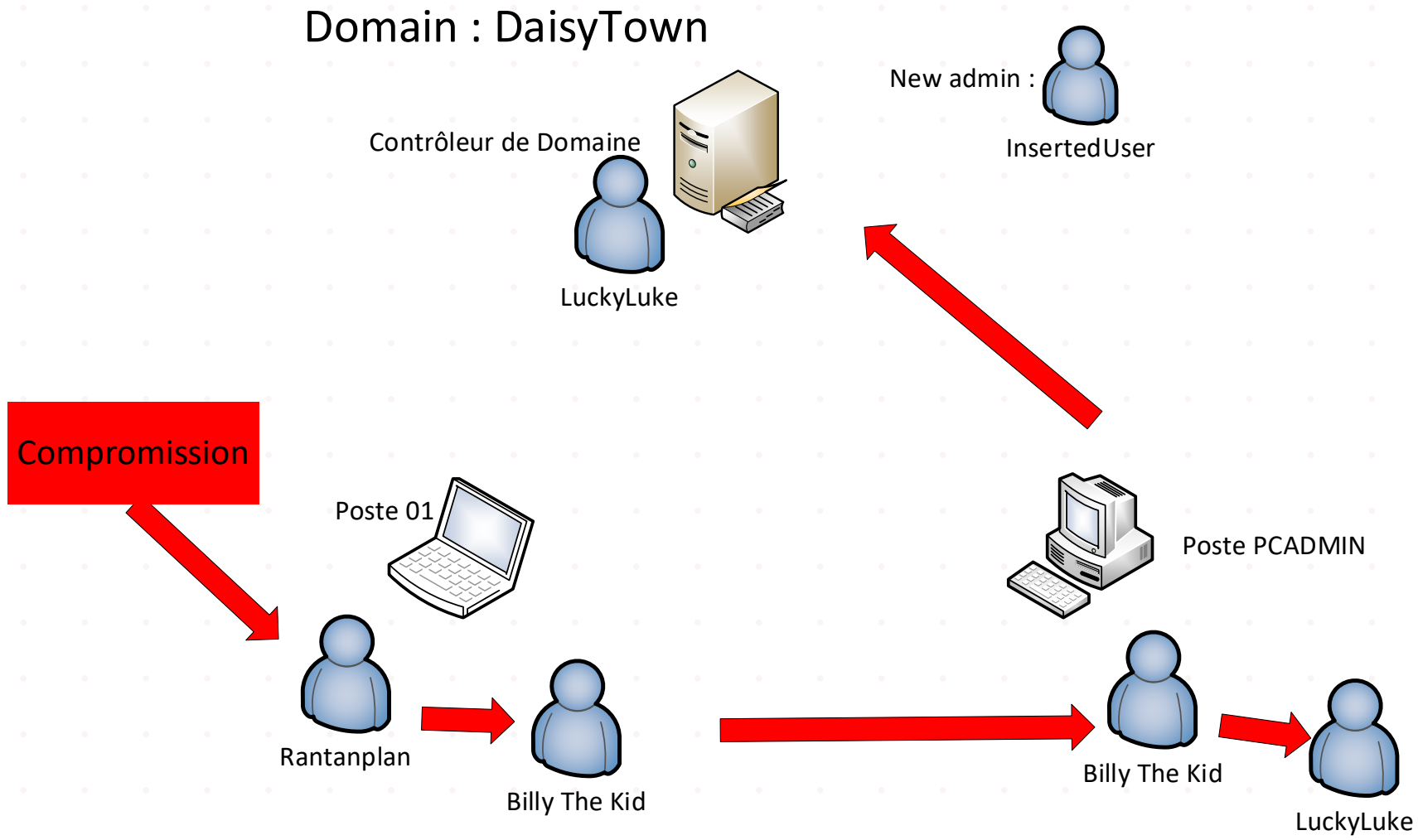
20220226_mesures-cyber-preventives-prioritaires.pdf (ssi.gouv.fr)

Se tenir informer et se former

- Blue Team vs Red Team
- Scénarios d'attaque / défense
- Permet d'entrainer les équipes
- A mettre en œuvre afin de tester :
    - Vigilance et Réactivité
    - Utilisation des outils de détection
    - Processus d'investigation
    - Communication

Illustration

Microsoft Defender for Identity Security Alert lab tutorial overview | Microsoft Docs



Il existe même des tutos en ligne

- **Cobalt Strike**

CobaltStrike

MANUALS_V2

Active Directory

I Этап. Повышение привелегий и сбор информации

1. Начальная разведка

1.1. Поиск дохода компании

Находим сайт компании
В Гугле: САЙТ + revenue (mycorporation.com+revenue)
("mycorporation.com" "revenue")
чекать больше чем 1 сайт, при возможности
(owler, manta, zoominfo, dnb, rocketrich)

1.2. Определене АВ

1.3. **shell whoami** <===== кто я

1.4. **shell whoami /groups** --> мои права на боте (если бот пришол с синим моником)

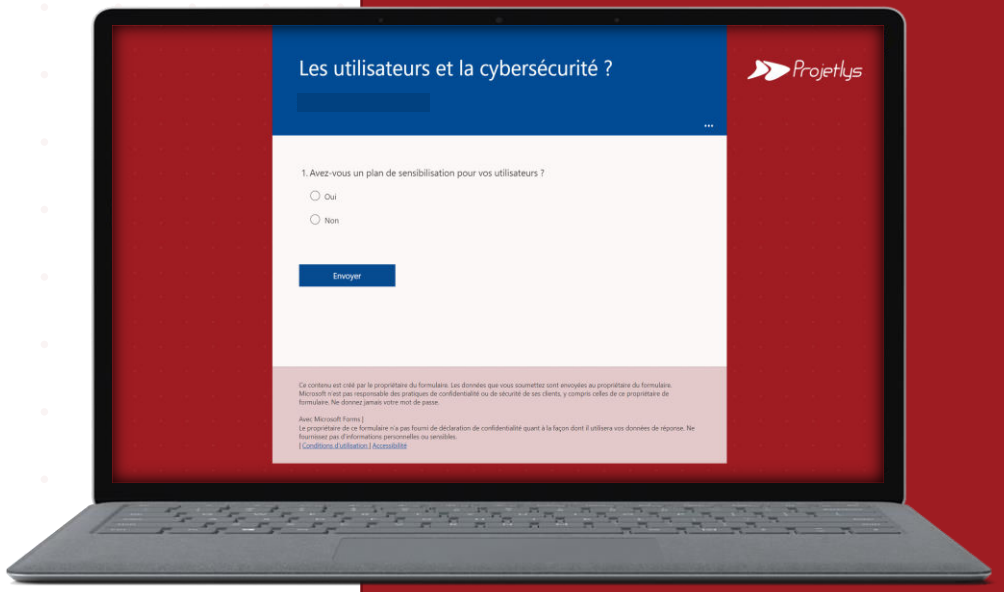
1.5.1. **shell nltest /dclist:** <===== контреллеры домена

03. Sensibilisation des utilisateurs

SONDAGE

LES UTILISATEURS ET LA CYBERSÉCURITÉ ?

https://forms.office.com/r/0rA4PvgAXm



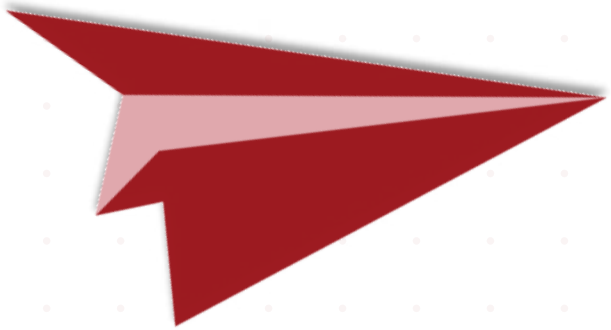
Projetlys

Projetlys

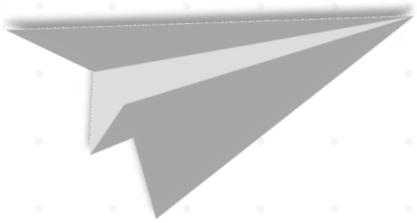
L'adoption des bonnes pratiques de sécurité passe en premier lieu par de la sensibilisation

PROSCI : modèle ADKAR®

Capacité à mettre en œuvre les bonnes pratiques en matière de cybersécurité et comportement requis quelque soit l'environnement dans lequel je me trouve



Ancrage des bonnes pratiques dans le temps et évolution de mon comportement en fonction des nouvelles menaces



Volonté de changer, pourquoi est-ce important de me protéger y compris à titre individuel, quels sont les risques encourus à ne pas le faire

Apprentissage des bonnes pratiques en matière de cybersécurité, Posture à adopter face à une menace

Sensibilisation aux enjeux de la cybersécurité à l'échelle de l'entreprise

Les étapes clés de notre démarche

1.

Contextualisation, cadrage, évaluation de la maturité des utilisateurs en matière de sécurité

2.

Simulation d'une campagne de phishing OU attaque brute-force

3.

Campagne de communication, webinar d'information, mise à disposition d'une fiche ou guide de bonnes pratiques

4.

Sensibilisation des utilisateurs finaux autour de formations interactives

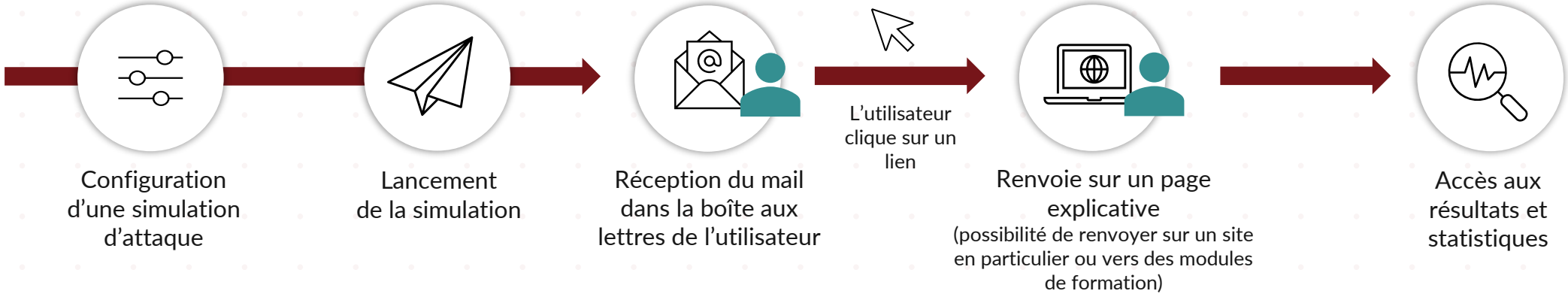
5.

Mise en place de **KPI** pour suivre l'évolution des bonnes pratiques et prochaines étapes

6.

Simulation d'une campagne de phishing OU attaque brute-force

Simulation d'attaque : Apprentissage



- Intégrer à Microsoft Defender
- Prise en main simplifié
- Intégrer cet exercice dans une démarche d'accompagnement et sensibilisation de vos utilisateurs
- Connaître la maturité des utilisateurs et proposer une démarche adaptée

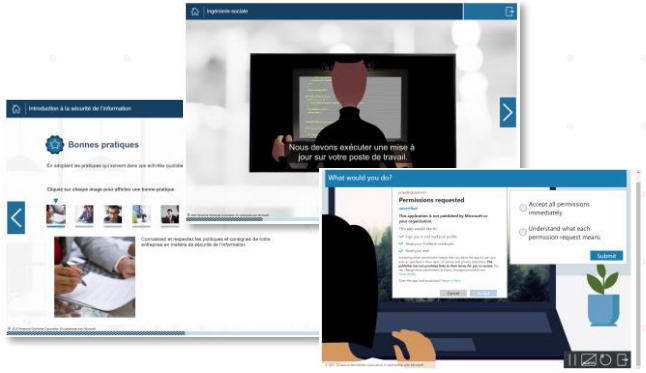
Sensibilisation des utilisateurs

COMMUNICATION DE MASSE

Communication en 3 temps sur différentes thématiques

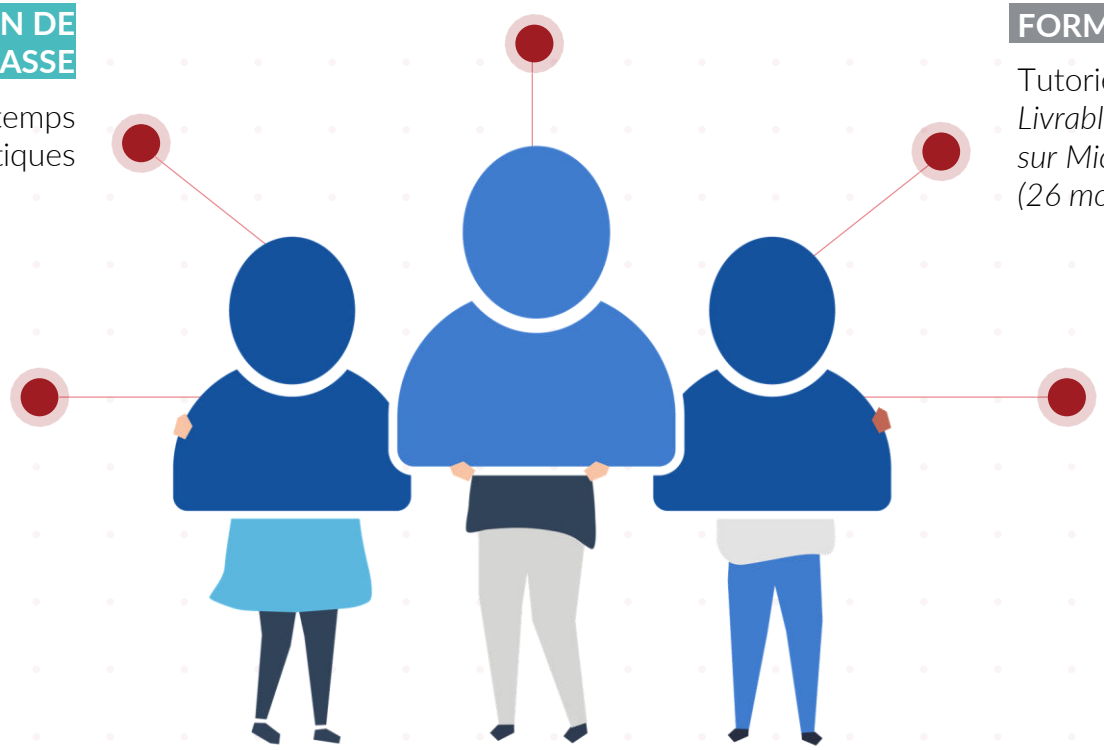
LIVRABLES PEDAGOGIQUES

Mise à disposition d'une fiche/guide de bonnes pratiques



FORMATIONS CIBLEES

Tutoriels vidéos interactifs
Livrables existants disponibles sur Microsoft Defender
(26 modules disponibles)



COMMUNICATION DE MASSE

Webinar d'information avec l'ensemble des utilisateurs

FORMATIONS CIBLEES

Sessions de formations par groupe :

- L'environnement du poste de travail
- L'utilisateur et ses identités
- Le télétravail

Quiz interactifs par sessions

Simulation d'attaque

Microsoft Defender

Collecte des informations d'identification

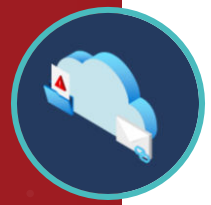
Persuader l'utilisateur à entrer son nom d'utilisateur et son mot de passe

Pièce jointe malveillante

Lorsque l'utilisateur ouvre la pièce jointe d'un mail. Un code s'est exécute pour aider l'attaquant à compromettre l'appareil de la cible.

Lien dans la pièce jointe

Présence d'une URL dans une pièce jointe de l'e-mail. L'URL dans la pièce jointe suit la même technique que la collecte des informations d'identification.



Lien vers un programme malveillant

Hébergement de la pièce jointe sur un site de partage de fichiers connu. Lorsque la cible clique sur l'URL, un code s'est exécute pour aider l'attaquant à compromettre l'appareil de la cible.

URL

L'URL malveillante dans le message permet à l'utilisateur d'accéder à un site web familier qui s'exécute en mode silencieux et/ou installe le code sur l'appareil de l'utilisateur.

04. La sécurité chez Projetlys

La force de nos équipes

Cyber Sécurité

L'équipe Change/Adoption

Des consultants spécialistes qui accompagnent l'adoption des solutions Microsoft 365, afin d'encourager le déploiement et l'adoption des nouveaux usages pour l'ensemble des collaborateurs d'une organisation.

Projetlys

CYBER SÉCURITÉ

14

24

L'équipe Technique

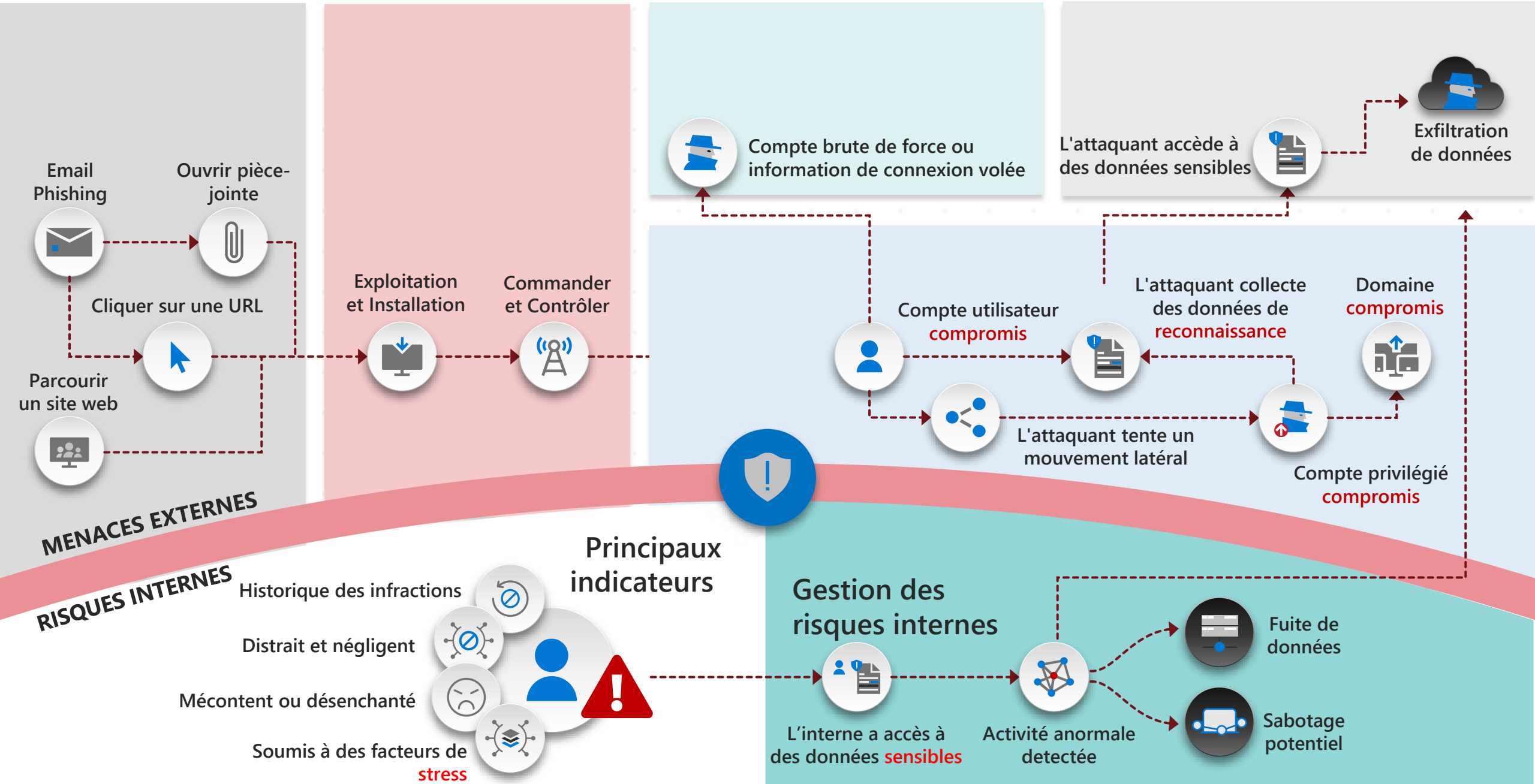
Des consultants spécialistes qui accompagnent au déploiement des différentes solutions Microsoft 365.

Certification MS-500: Microsoft 365 Security Administration
Certification AZ-500: Microsoft Azure Security Technologies
Certification SC-200 : Microsoft Security Operations Analyst
Certification SC-300 : Microsoft Identity and Access Administrator
Certification SC-400 : Microsoft Information Protection Administrator
Certification MS-100: Microsoft 365 Identity and Services
Certification MS-101: Microsoft 365 Mobility and Security

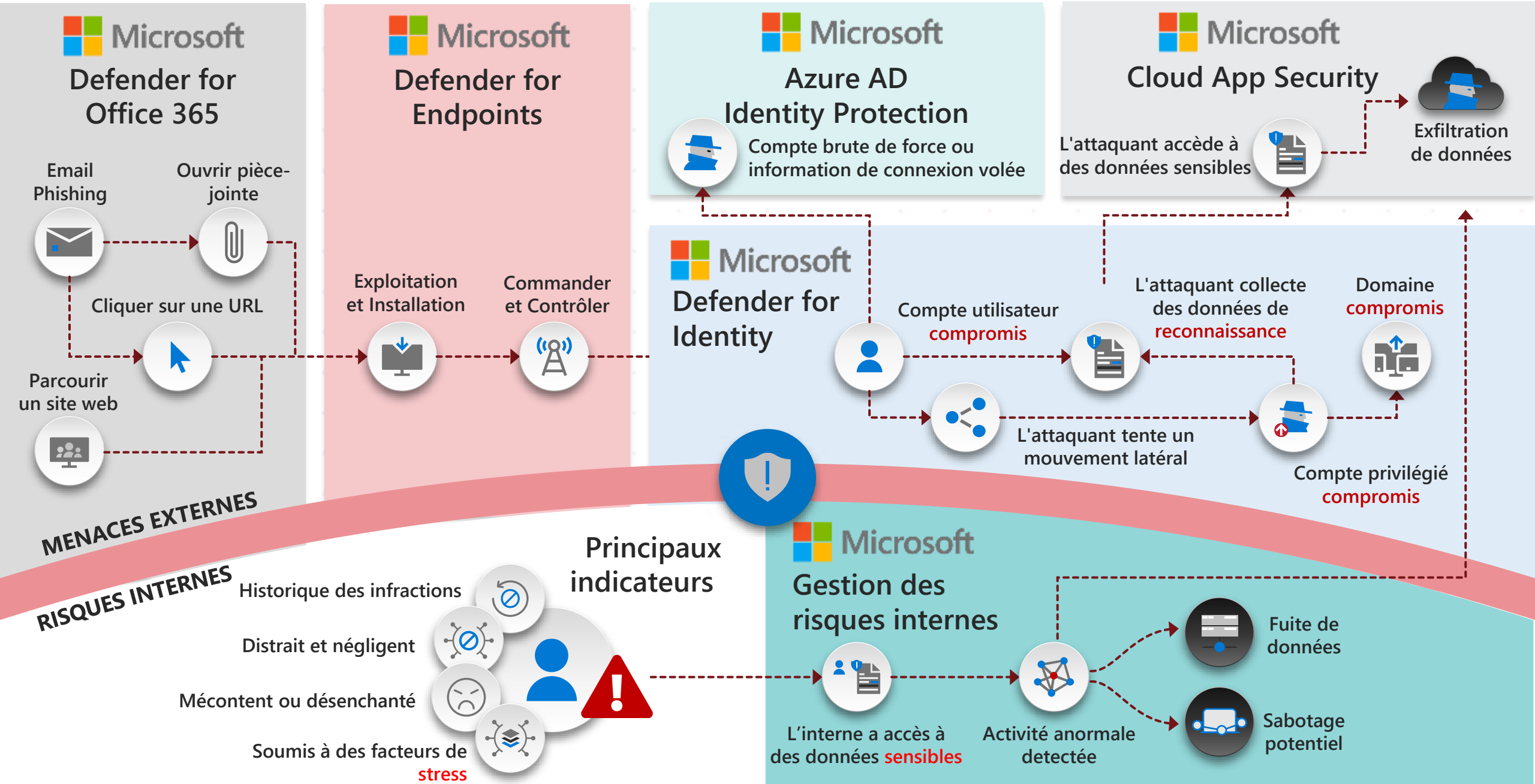
Exemples de nos domaines d'intervention

- Sensibilisation des utilisateurs
- Définition des règles de sécurité et plan de mise en œuvre
- Elaboration et mise en œuvre de la classification des documents
- Security Morning Check
- Définition et mise en œuvre du least privilege
- Conception et déploiement d'Active Directory Tiering Model
- Déploiement des solutions de sécurité Microsoft Defender
- Audits AD, conception et suivi du plan de remédiation
- Déploiement du SIEM
- Formation, transfert de compétences

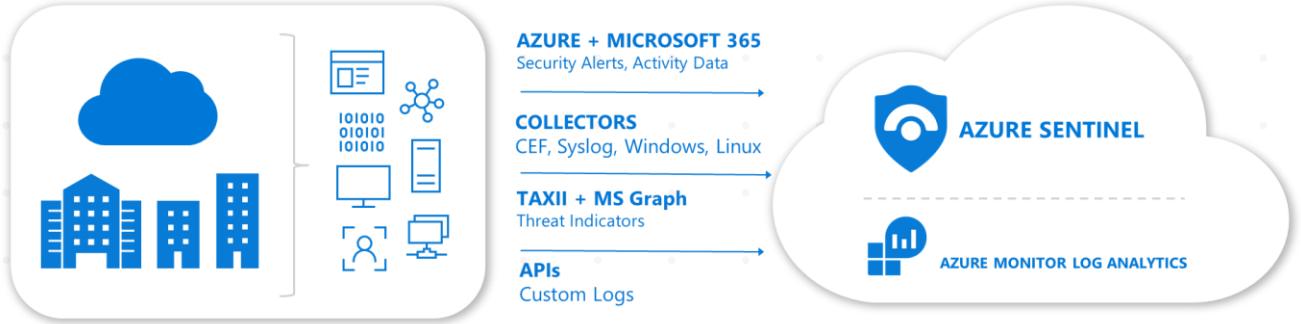
Protection complète tout au long de la kill chain



Protection complète de Microsoft tout au long de la kill chain

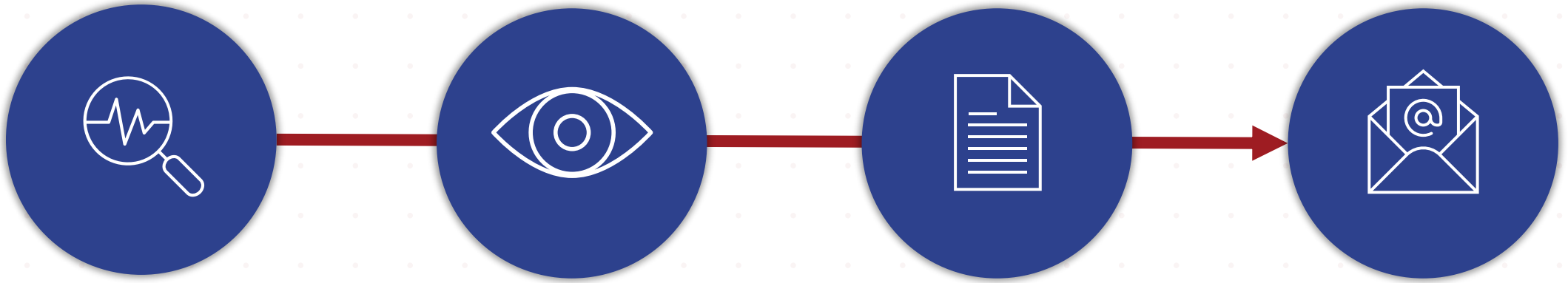


Expérience unifiée



Communauté + experts sécurité Microsoft

Morning Check

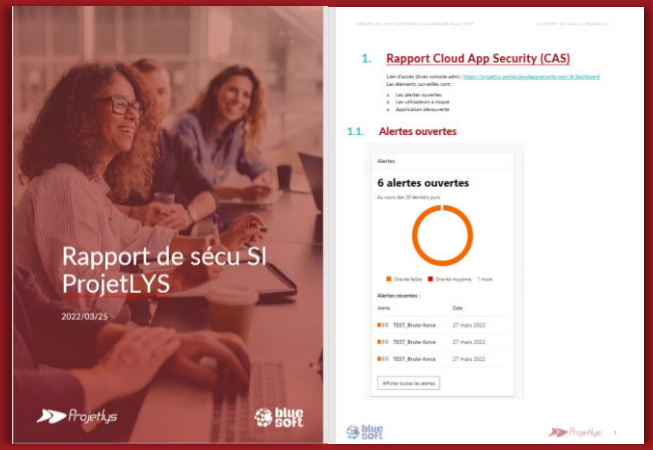


Collecte des informations

Analyse par le service client

Rédaction du rapport

Envoi du rapport par email



Rapport envoyé

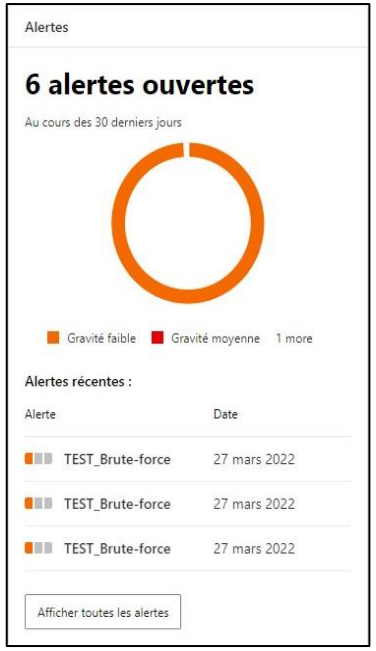
Points abordés dans le rapport

1. Rapport Cloud App Security (CAS)
2. Rapport Microsoft Defender 365
3. Check Phishing/ Malware
4. Utilisateurs à risque Azure
5. Patching des postes et vérification des comptes AD
6. Backup
7. Rapports quotidiens MS Identity
8. Résumé du jour
9. Alerte en cours

Rapport Cloud App Security

MORNING CHECK

Alertes ouvertes



Apps découvertes

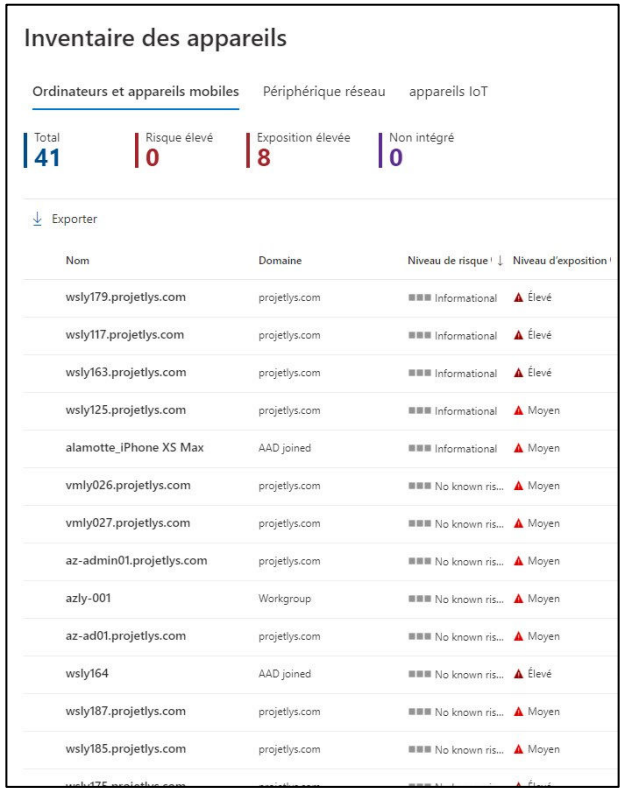
Utilisateurs « à risque »

Projetlys

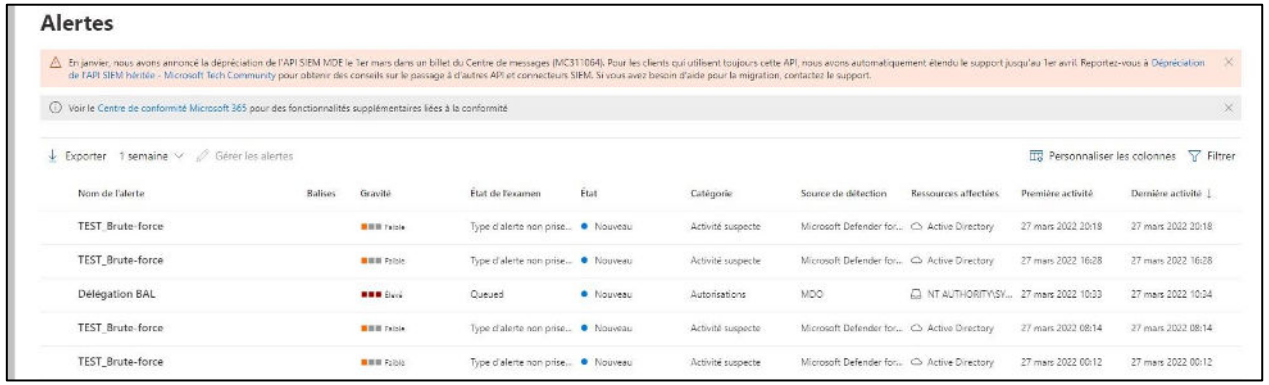
Rapport Microsoft Defender 365

MORNING CHECK

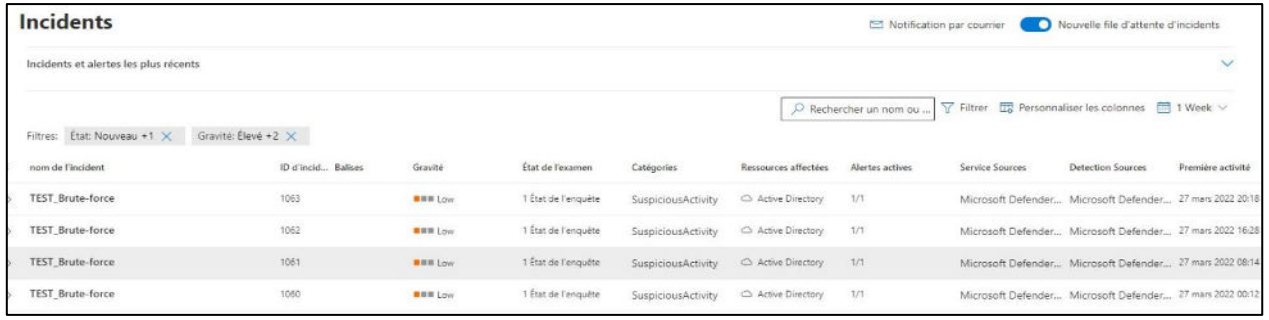
Les points de terminaison



Liste des alertes



Liste des incidents

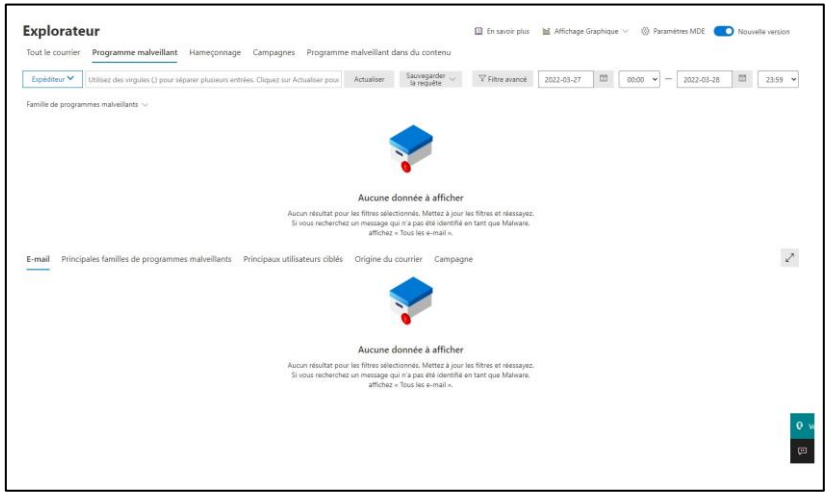


Projetlys

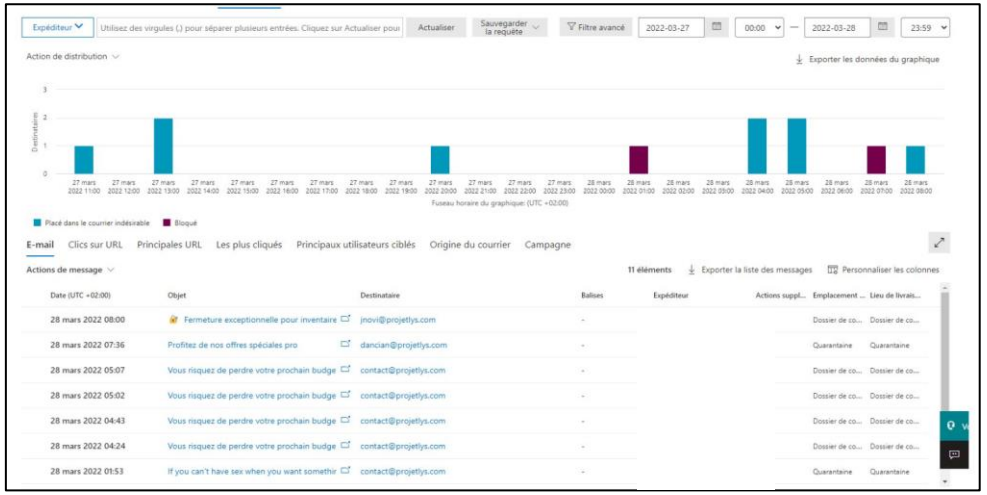
Check Phishing/Malware

MORNING CHECK

Malware



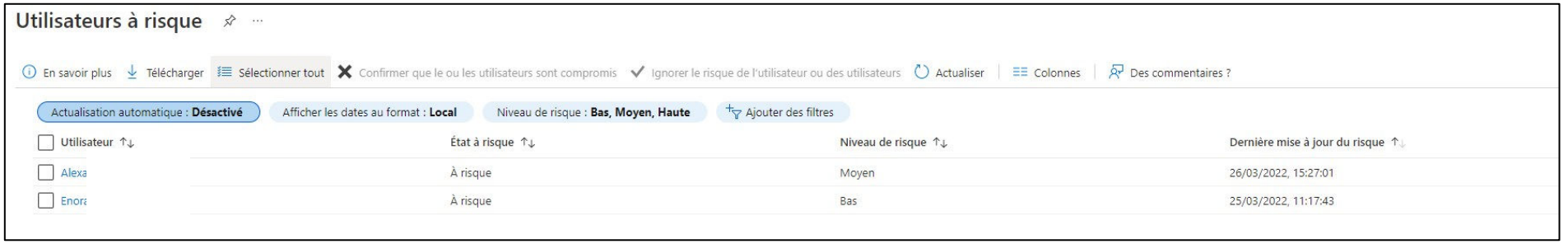
Phishing



Projetlys

Utilisateurs à risque Azure & Rapport MS Identity

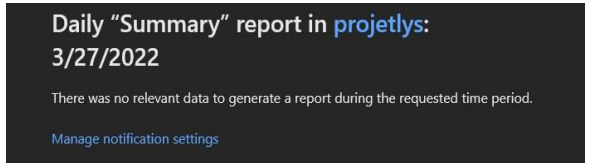
MORNING CHECK



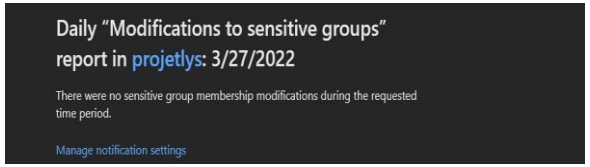
Lateral movements paths to sensitive accounts

Password exposed in cleartext

Summary



Modification to sensitive groups



Projetlys

Patching & Backup

MORNING CHECK

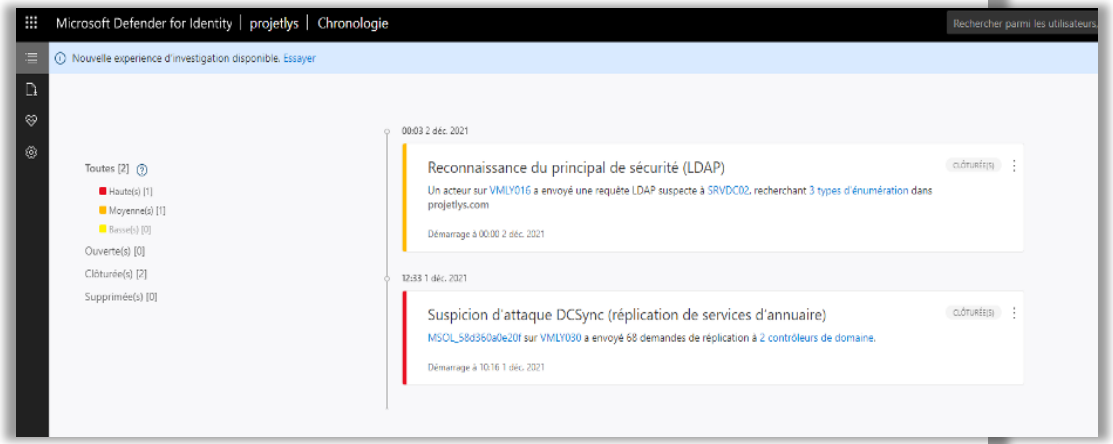
Patching des postes (mensuel)
Poste en retard : 3

Patching des serveurs (mensuel)
Total serveur on premise à jour : 95%
VM Azure à mettre à jour

Backup
Sauvegarde Barracuda

DATE	TEAMS	EXCHANGE	ONEDRIVE	SHAREPOINT
28/03/2022	OK	OK	OK	OK

Vérification des comptes AD
Microsoft Defender for Identity



Résumé quotidien & Alertes

MORNING CHECK

8. Résumé du jour

Voici donc un résumé rapide des alertes ou utilisateurs nécessitant une action :

- Cloud App Security :
  - 6 alertes ouvertes
    - Clos : Brute Force sur compte désactivé
    - Clos : Brute Force sur compte désactivé
  - 1 utilisateur au-dessus de la normal
    - [redacted] - Alerte Brute Force > Failed Log On (devrai revenir à la normal dans 7 jours)
- Defender 365 :
  - Incidents
    - Clos : Brute Force compte sur compte désactivé> Failed Log on
  - 1 Alerte :
    - Clos : Brute Force compte [redacted] Failed Log on
    - Clos : Délégation de BAL > Process auto-Exchange
  - Points de Terminaison :
    - RAS
  - Checking
    - Malware : RAS
    - Phishing : RAS
- Utilisateurs à risques Azure :
  - [redacted]
- Sauvegarde
  - RAS
- Rapport quotidiens MS Identity
  - RAS

9. Alerte en cours

RCA : Alerte en cours d'investigation (RCA).docx

Listing en cours :

- RAS

RCA :

- Formaliser l'incident
- Collecter les preuves
- Identifier les facteurs
- Déterminer la cause principale
- Décrire les mesures prises
- Décrire le plan de remédiation

Projetlys

Questions ?

Projetlys

Merci !

www.bluesoft-group.com

www.projetlys.com

bluesoft