

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



---

Mardi 5 avril 2022



# 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 Projellys

---

# 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 à **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



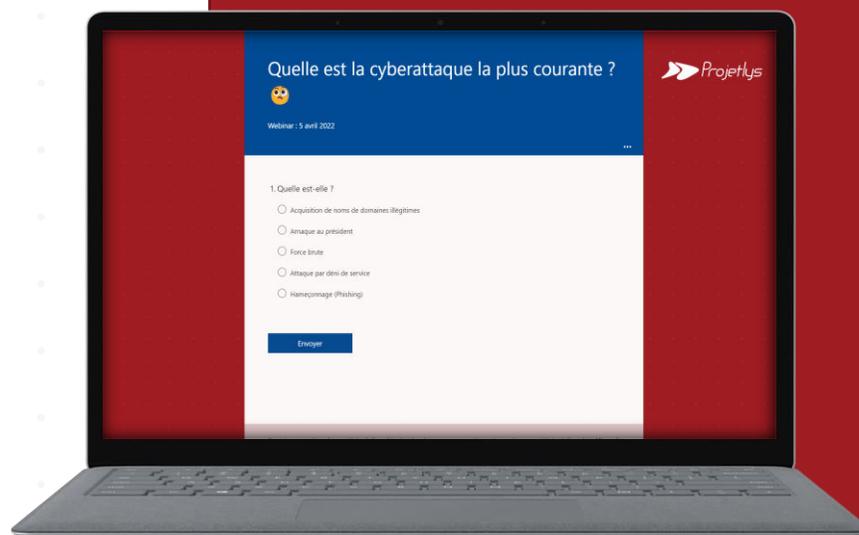


<https://forms.office.com/r/uSbea4aJKB>

SONDAGE

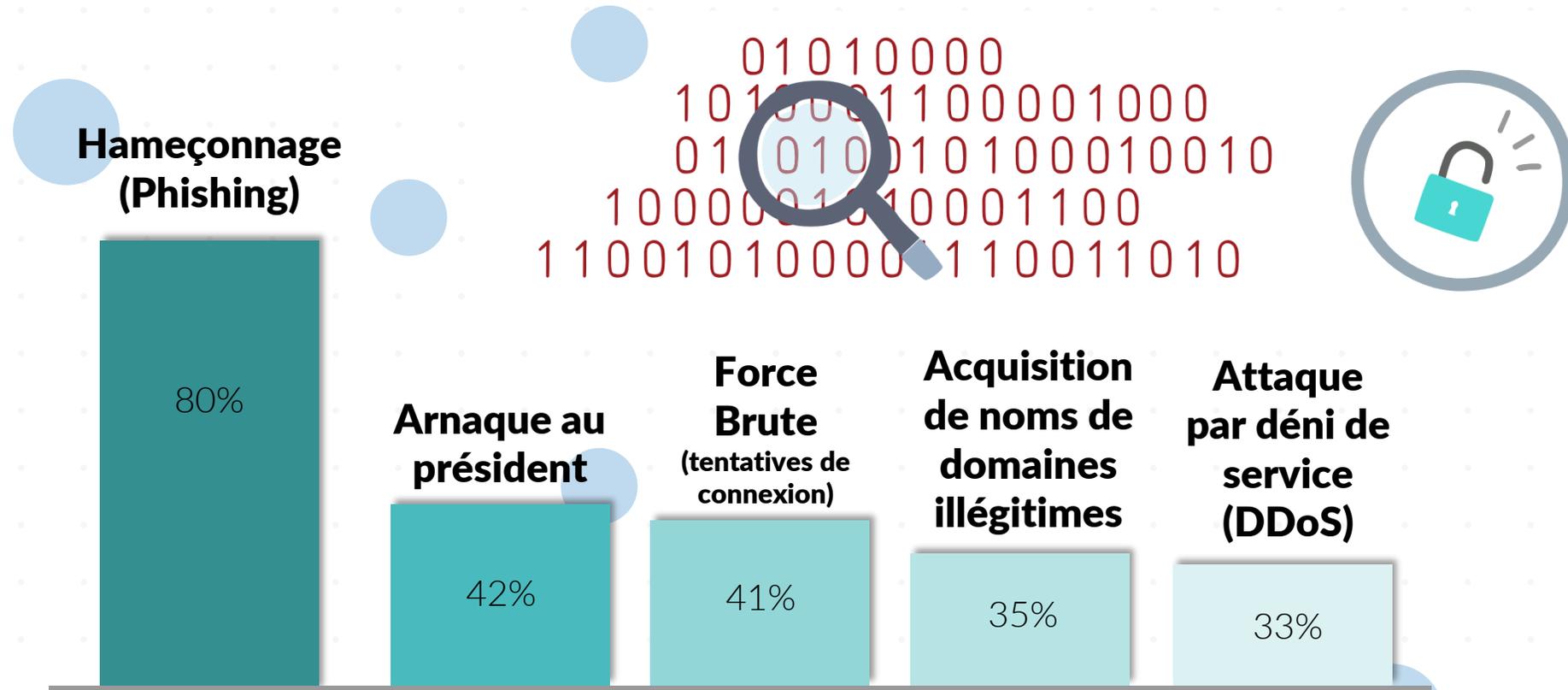
# QUELLE EST LA CYBERATTAQUE LA PLUS COURANTE ?

Une petite idée ?



# Les cyberattaques

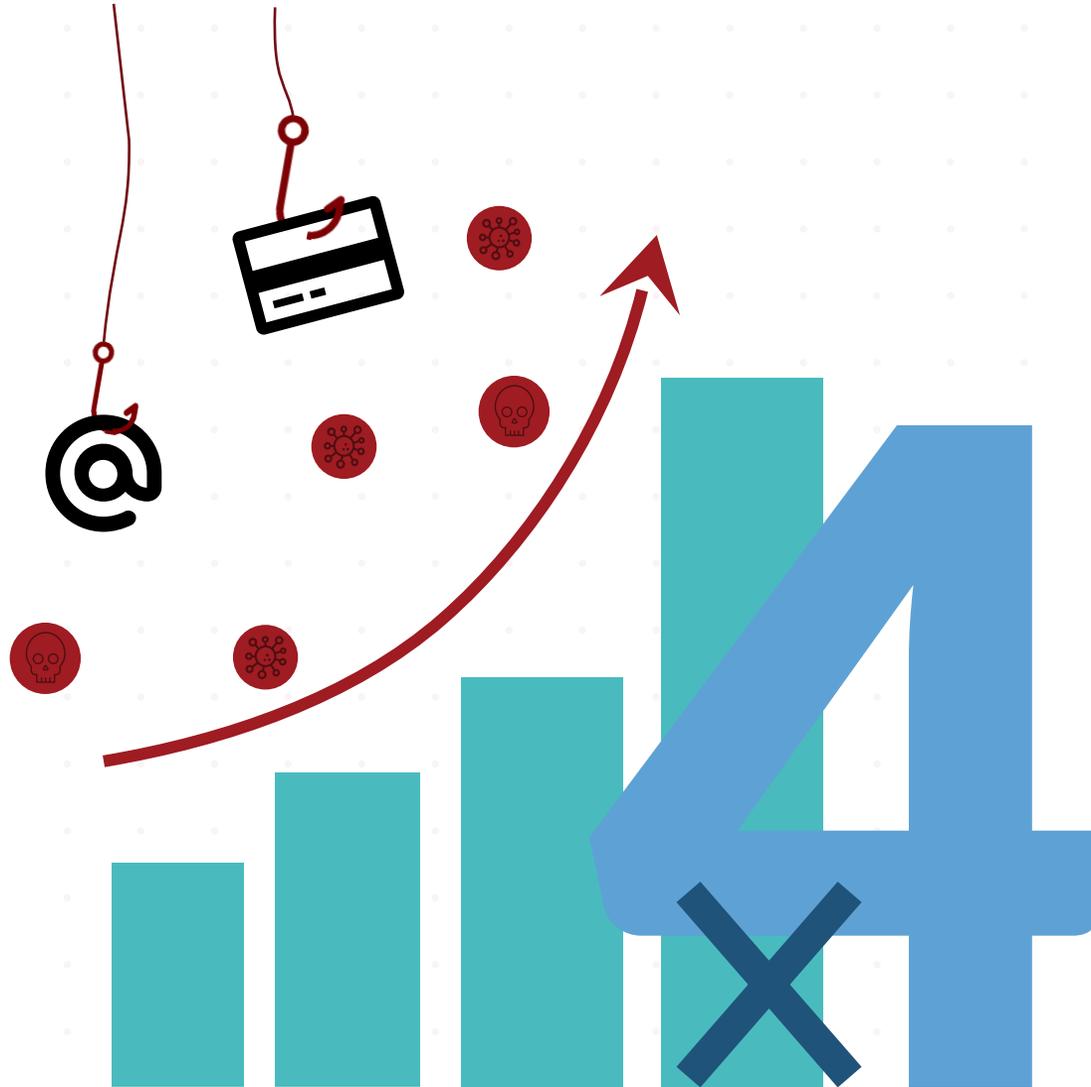
Les plus courantes contre les entreprises en 2020



\*Plusieurs réponses possibles. Sélection des plus fréquentes.

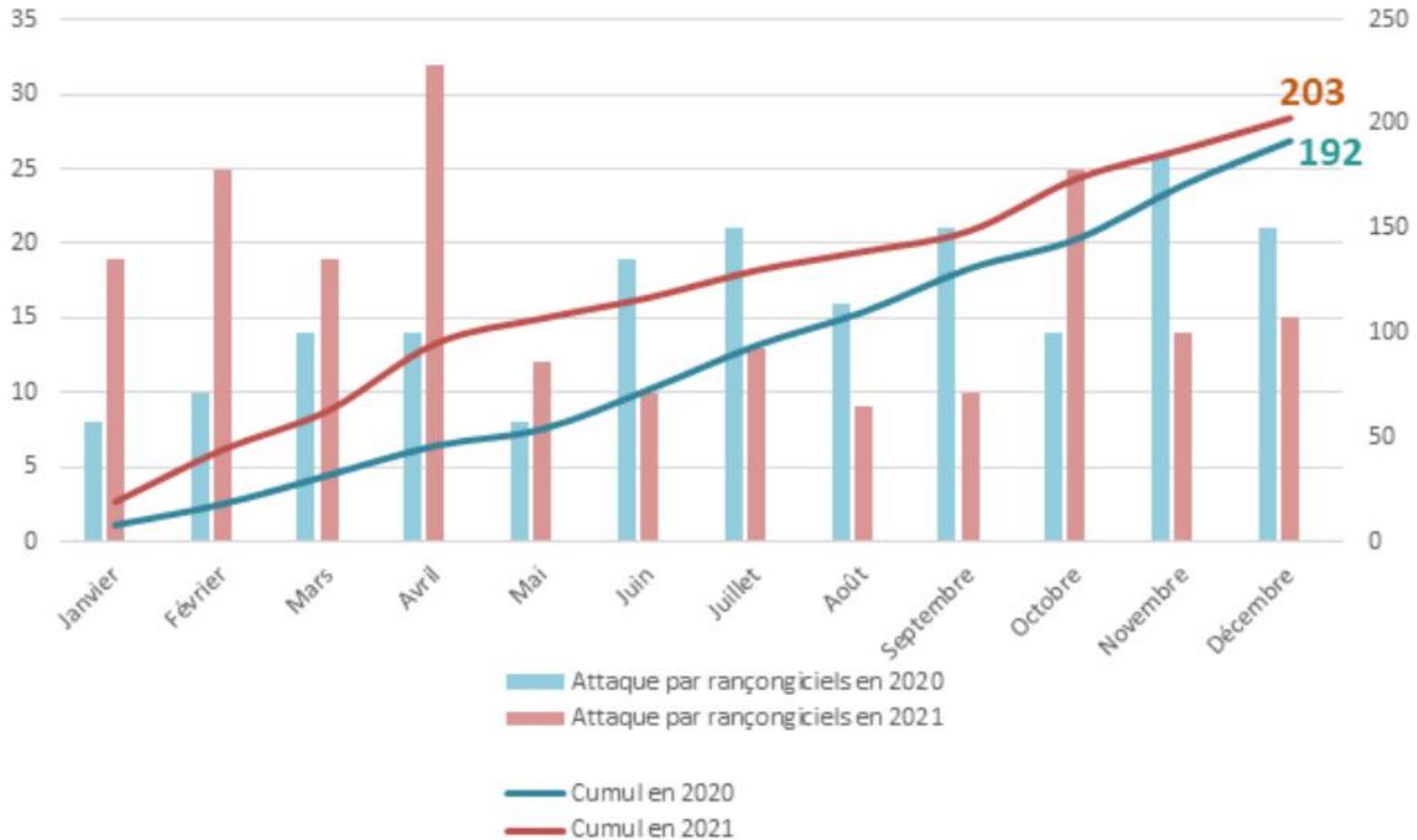
(source: statista)

# 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%

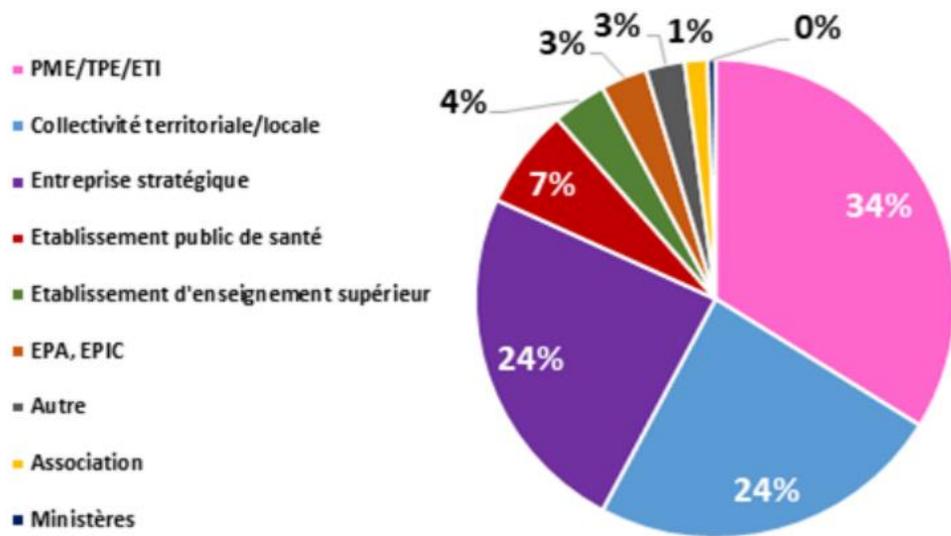
jugent que les utilisateurs finaux ne sont pas équipés ou formés pour le télétravail  
(source: Proofpoint)

80%

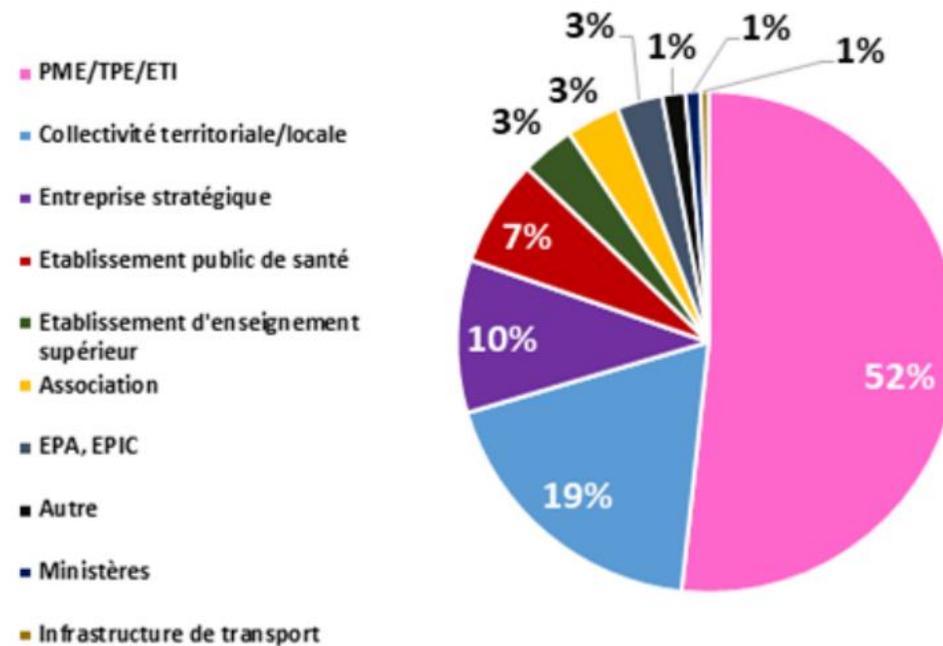
des cyberattaques viennent de la gestion des identités



# Répartition des entités victimes par rançonneur



2020



2021

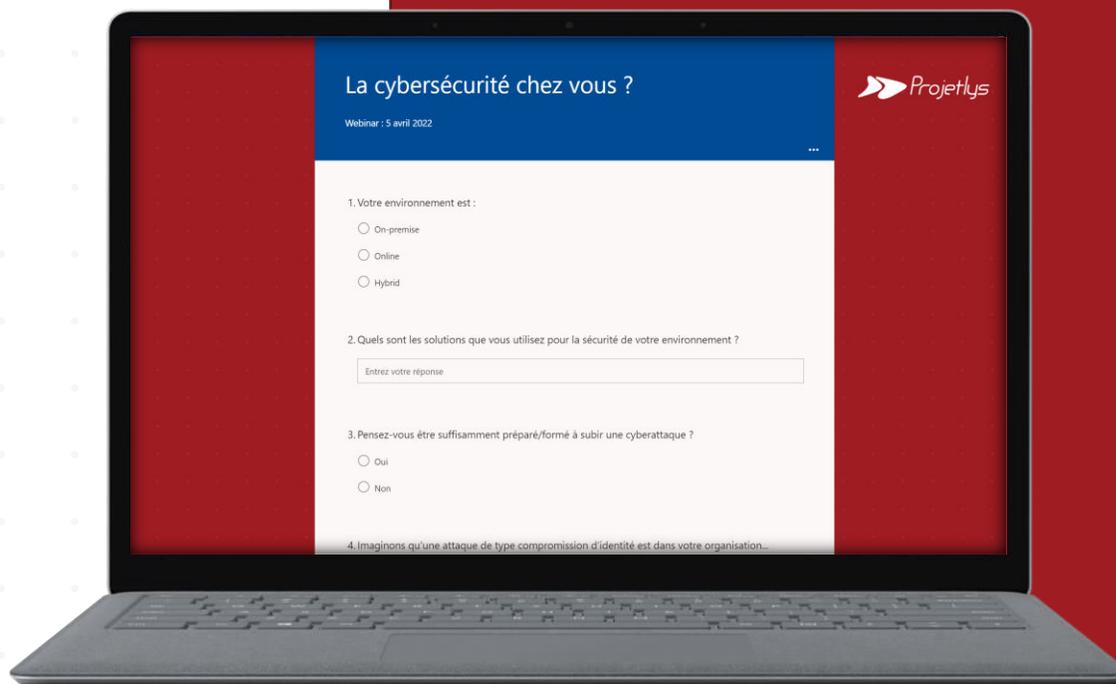
# 02. Comment renforcer rapidement et efficacement son SI ?

---

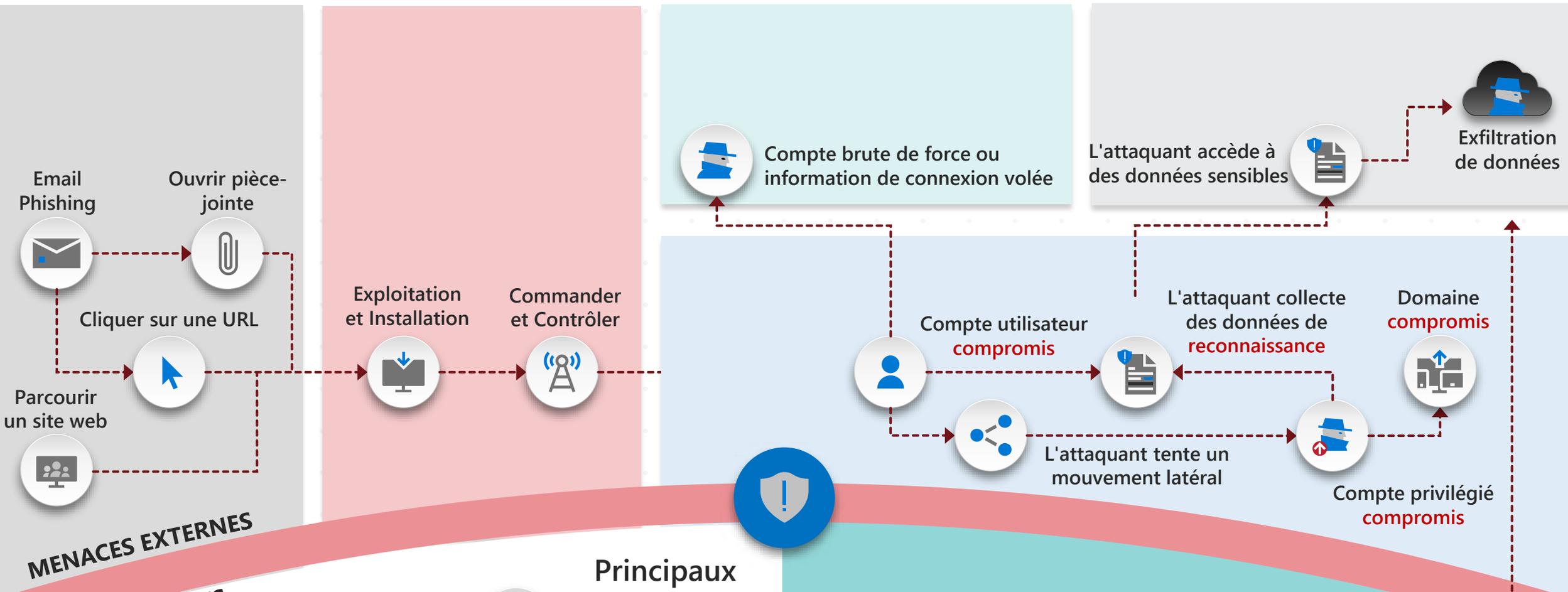


<https://forms.office.com/r/86pUb4tqVt>

# SONDAGE LA CYBERSÉCURITÉ CHEZ VOUS ?



# Protection complète tout au long de la kill chain



**MENACES EXTERNES**  
**RISQUES INTERNES**

### Principaux indicateurs

- Historique des infractions
- Distrait et négligent
- Mécontent ou désenchanté
- Soumis à des facteurs de stress

### Gestion des risques internes

- L'interne a accès à des données sensibles
- Activité anormale détectée
- Fuite de données
- Sabotage potentiel

# Microsoft Zero Trust solution

## Utilisateur

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



Microsoft Azure AD



Defender for Identity



Defender for Endpoint



Microsoft Intune



## Périphérique

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

Vérifier explicitement | Moindre privilège | Accepter la brèche

Politique de sécurité et de conformité

Visibilité | Analyse | Automatisation



Azure Sentinel



Microsoft Information Protection



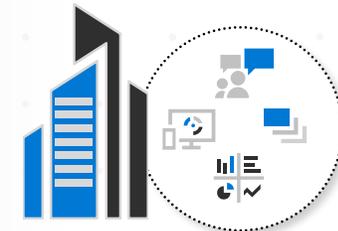
Microsoft Cloud App Security



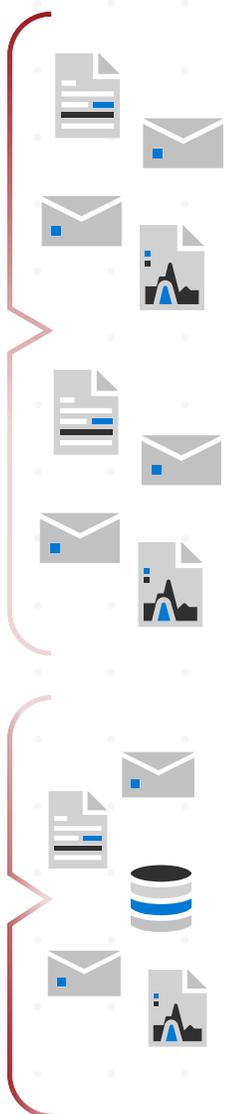
Microsoft Cloud



Cloud SaaS apps



On-premises & web apps

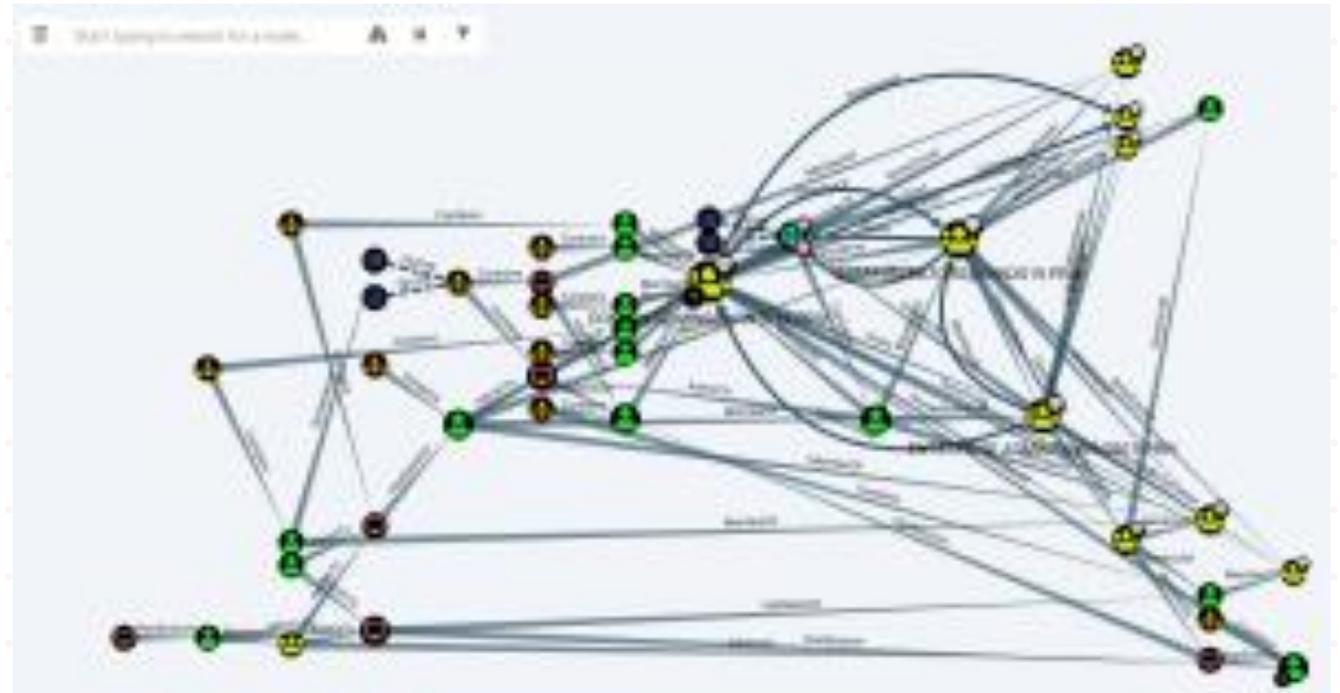


# Le mouvement latéral : définition

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

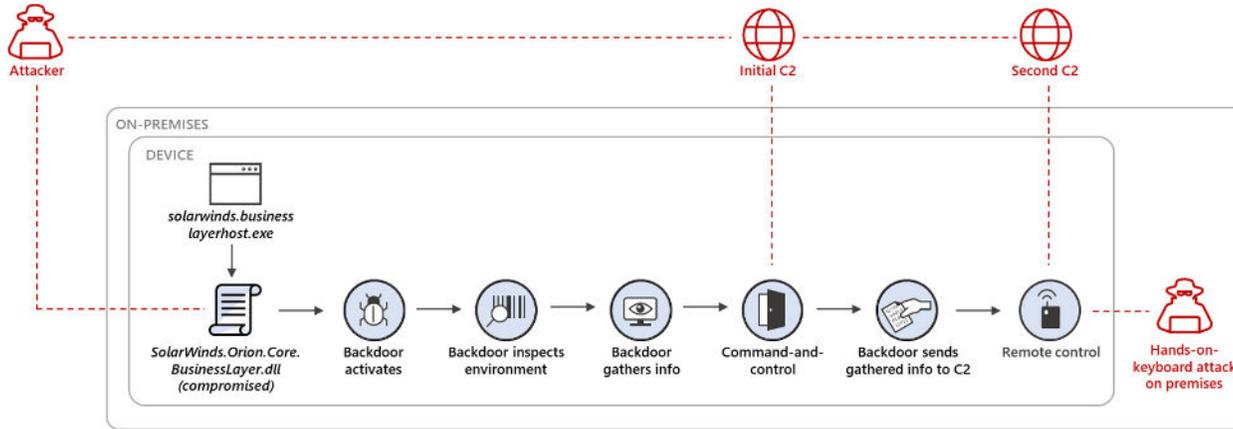
Utiliser des comptes non sensibles pour obtenir l'accès à des comptes sensibles dans votre réseau.

Exemple de cartographie avec BloodHound



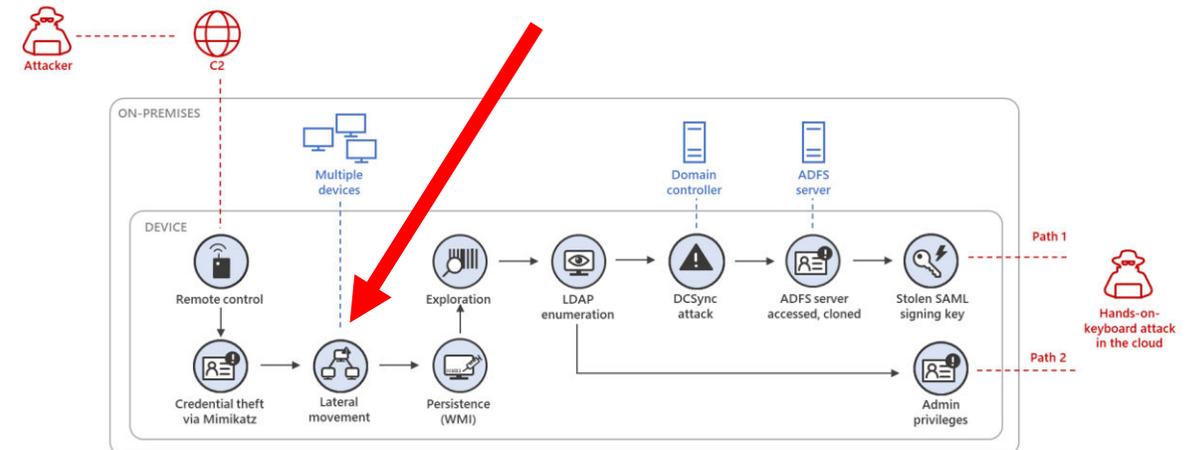
# Très souvent utilisé

## SOLORIGATE ATTACK Stage 1: Initial access and command-and-control



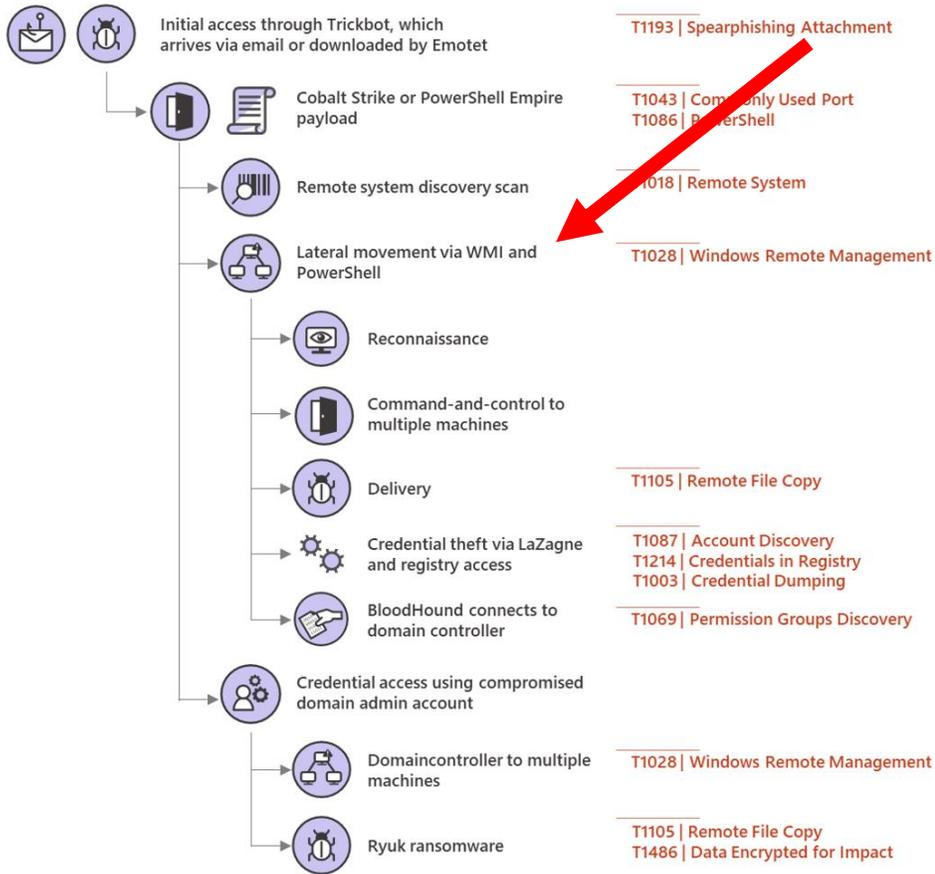
[Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security Blog](#)

## SOLORIGATE ATTACK Stage 2: Hands-on-keyboard attack on premises



# Très souvent utilisé

## Ryuk attack chain



## Doppelpaymer attack chain



# 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

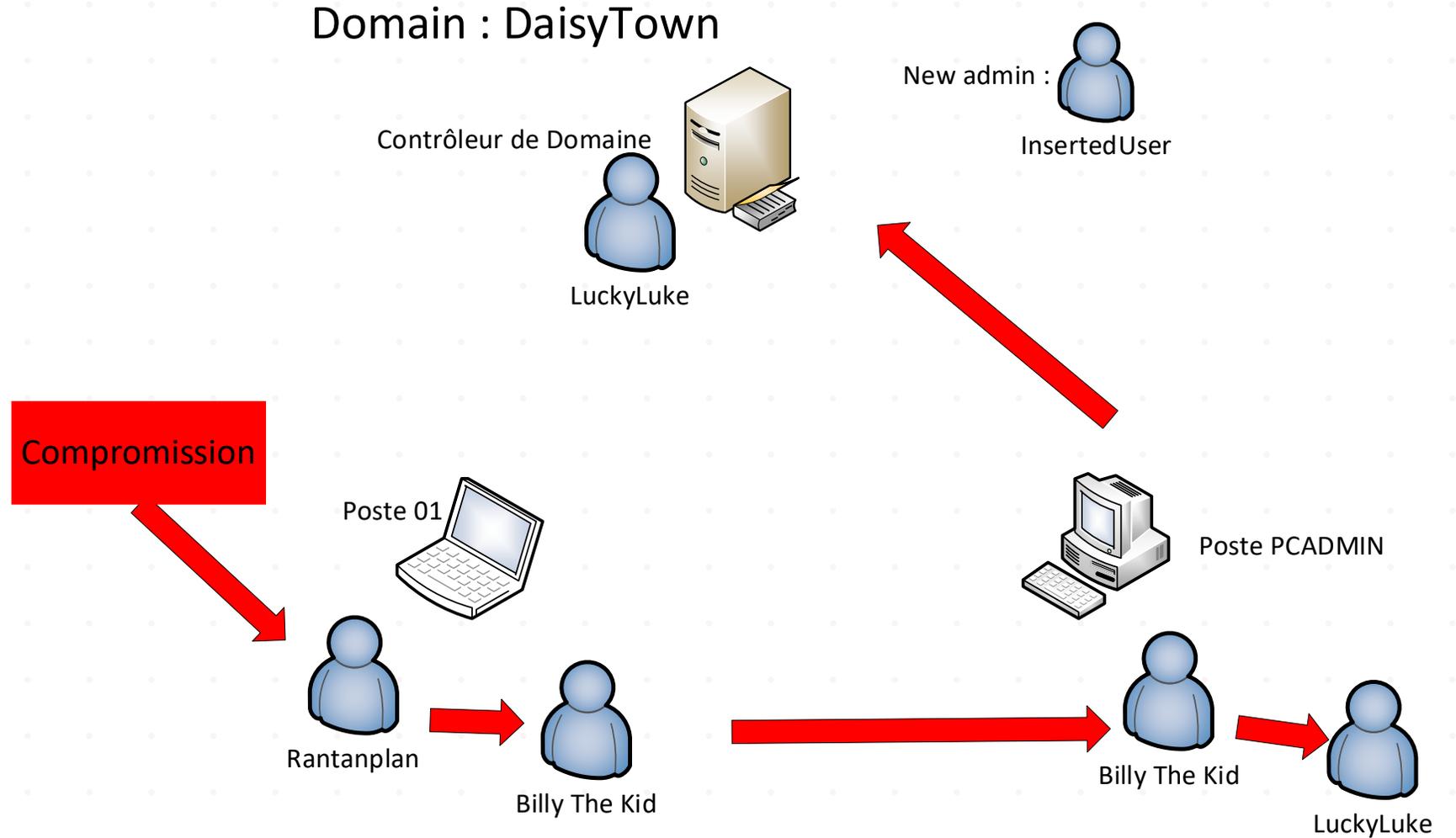
---

- Blue Team vs Red Team
- Scénarios d'attaque / défense
- Permet d'entraîner 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  
пришел с синим монитором)

1.5.1. `shell nltest /dclist:` <===== контроллеры домена



# 03. Sensibilisation des utilisateurs

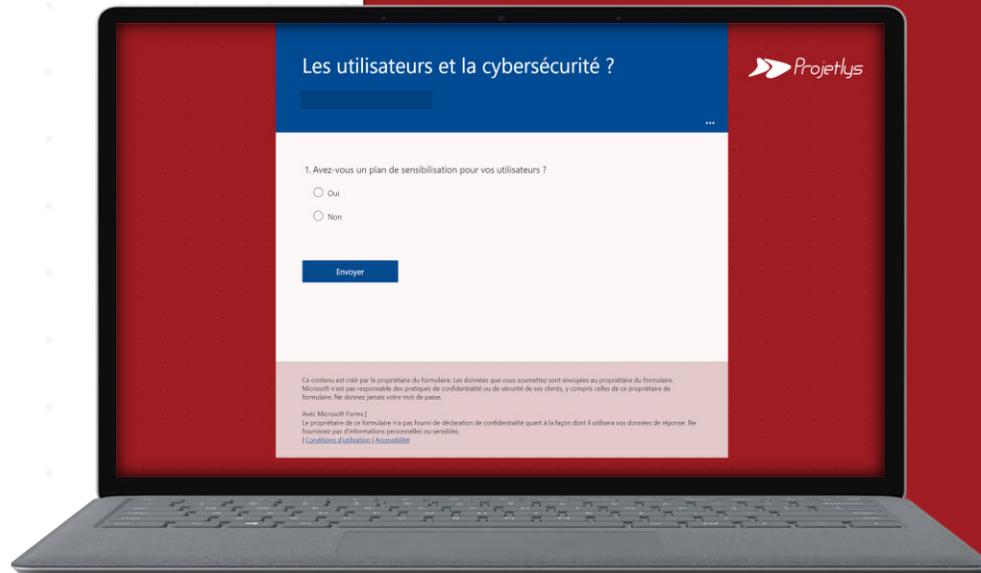
---



<https://forms.office.com/r/OrA4PvgAXm>

SONDAGE

# LES UTILISATEURS ET LA CYBERSÉCURITÉ ?



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

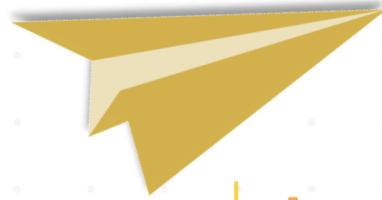
PROSCI : modèle ADKAR®



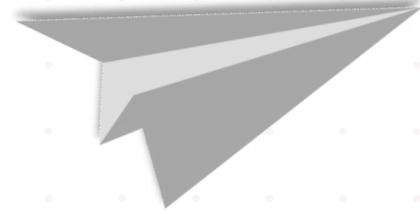
**Volonté** de changer, pourquoi est-ce important de me protéger y compris à titre individuel, quels sont les risques encourus à ne pas le faire



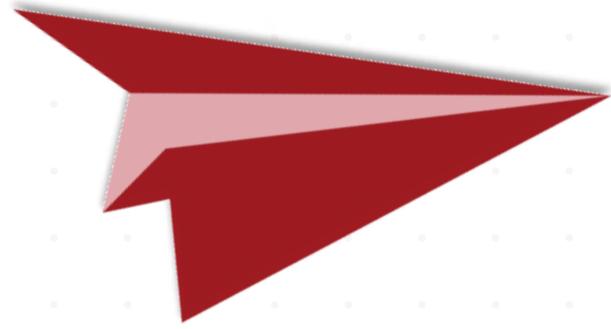
**Sensibilisation** aux enjeux de la cybersécurité à l'échelle de l'entreprise



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



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



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

# 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

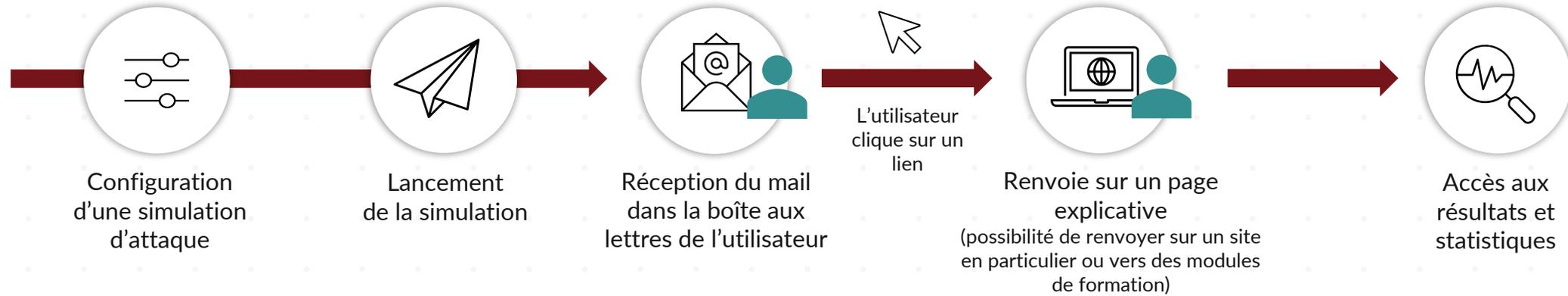


6.

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

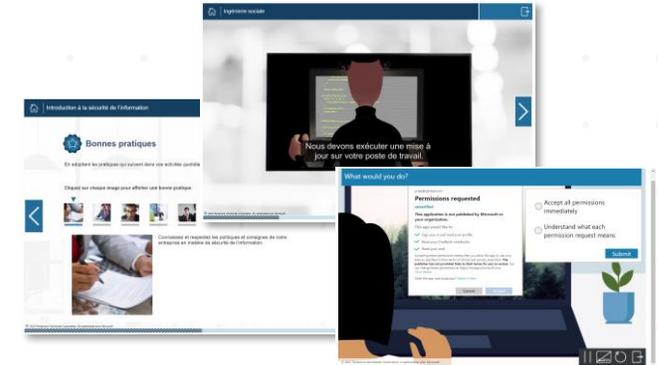
## COMMUNICATION DE MASSE

Webinar d'information avec l'ensemble des utilisateurs



## 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)*



## 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 exécuté 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 exécuté 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.



SecNum  
académie

ANSSI



Projetlys

CYBER  
SÉCURITÉ

14



### 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

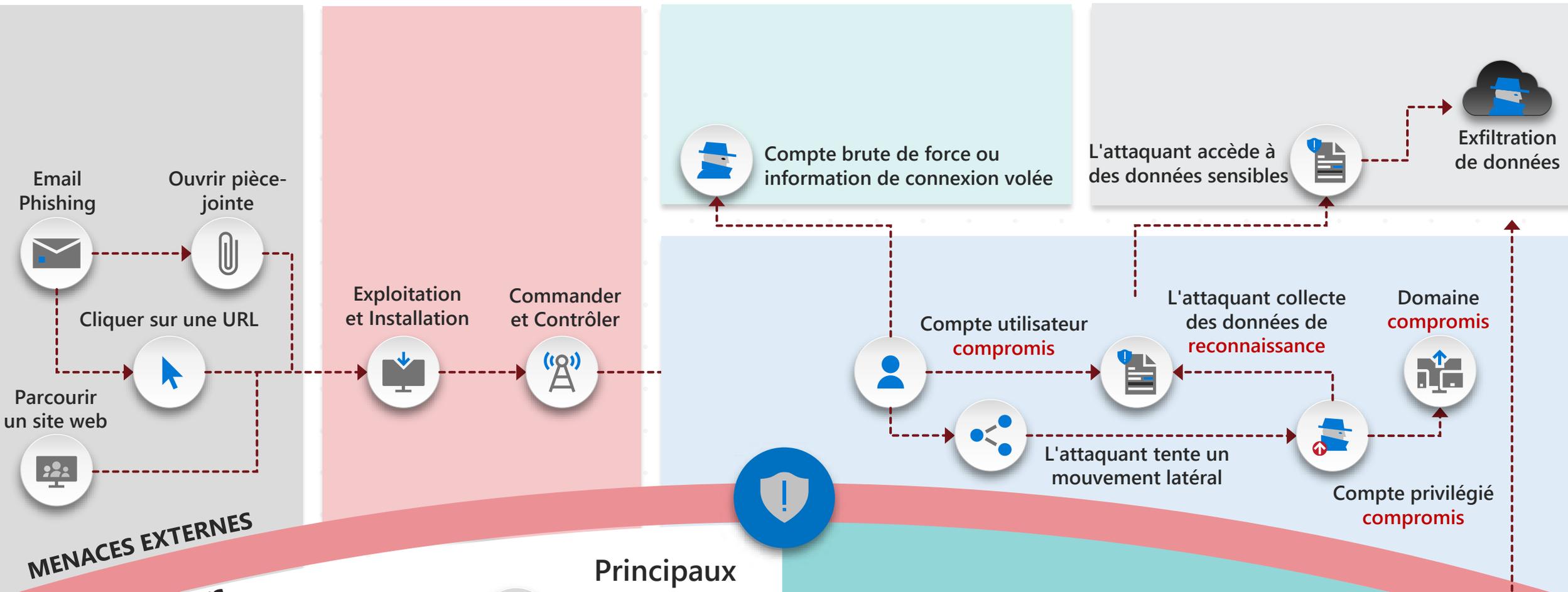
24

# 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



MENACES EXTERNES  
RISQUES INTERNES

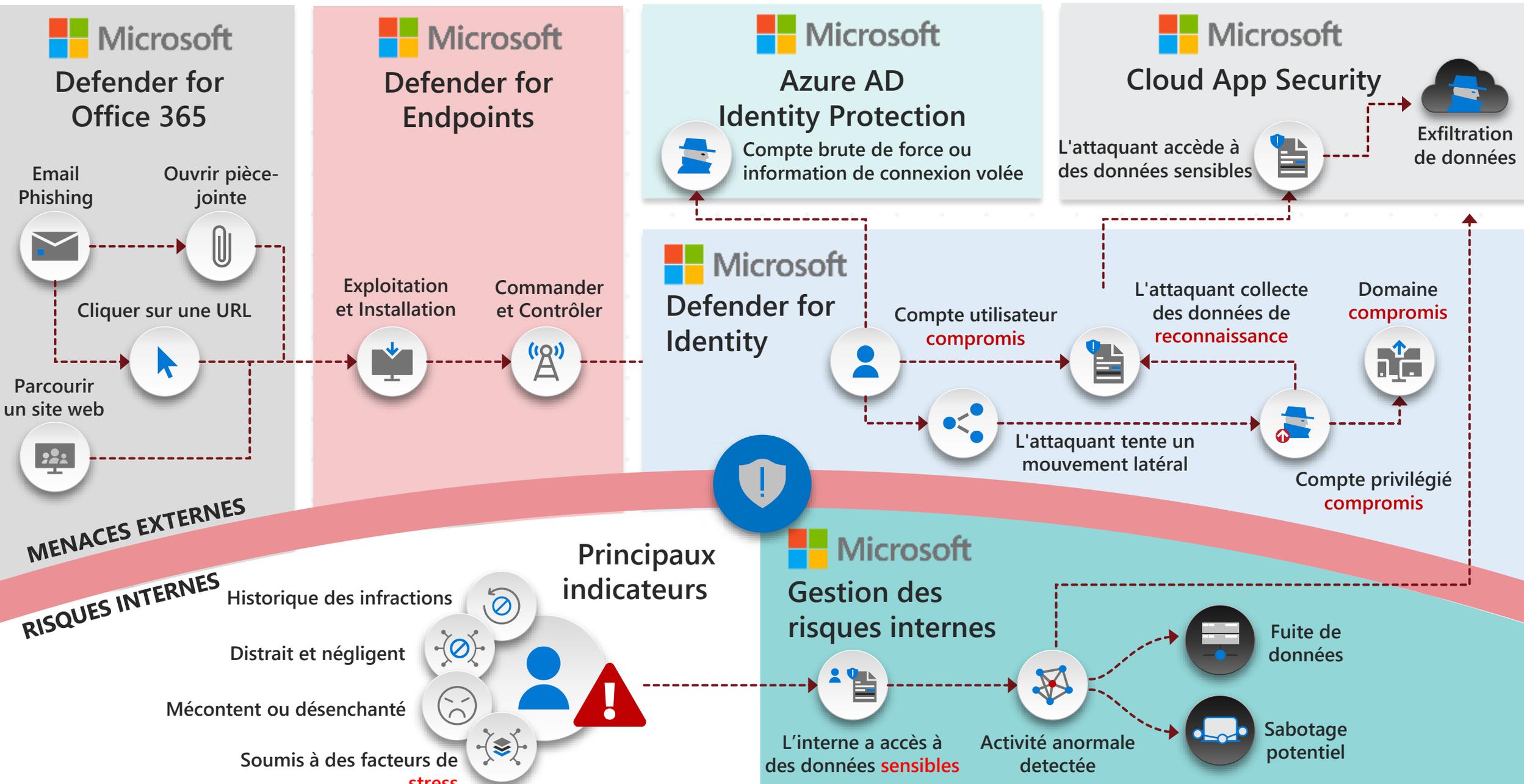
### Principaux indicateurs

- Historique des infractions
- Distrait et négligent
- Mécontent ou désenchanté
- Soumis à des facteurs de stress

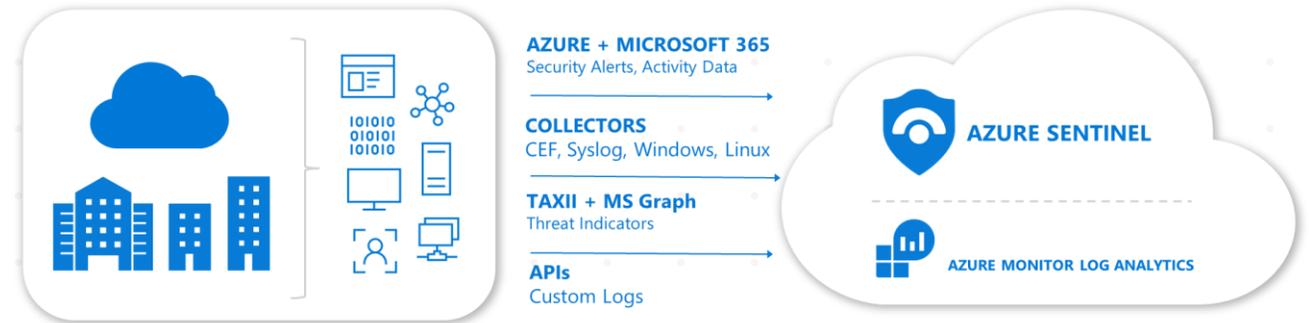
### Gestion des risques internes

- L'interne a accès à des données sensibles
- Activité anormale détectée
- Fuite de données
- Sabotage potentiel

# Protection complète de Microsoft tout au long de la kill chain

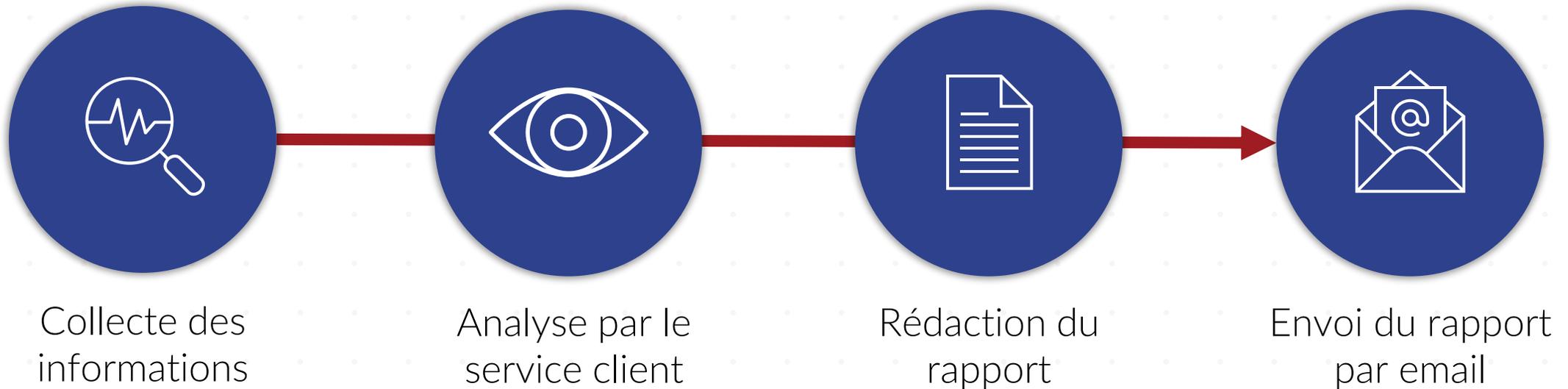


# Expérience unifiée



Communauté + experts sécurité Microsoft

# Morning Check



# 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  
envoyé

# Rapport Cloud App Security

## MORNING CHECK

### Alertes ouvertes



### Apps découvertes



### Utilisateurs « à risque »

Utilisateurs principaux à examiner

**85 utilisateurs à exami...**

La priorité d'enquête est calculée en fonction des alertes et des activités de l'utilisateur au cours des 7 derniers jours

Utilisateurs principaux à examiner :

Nom	Score de priorité d'investigation
Adm	267
Adm	58
Chris	46
Adm	40
Adm	38
Alexi	28
Gille	28

[Afficher tous les utilisateurs à examiner](#)

# Rapport Microsoft Defender 365

## MORNING CHECK

### Les points de terminaison

Inventaire des appareils			
Ordinateurs et appareils mobiles			
Total	Risque élevé	Exposition élevée	Non intégré
41	0	8	0
↓ Exporter			
Nom	Domaine	Niveau de risque ↓	Niveau d'exposition ↓
wsly179.projetyls.com	projetyls.com	Informational	Élevé
wsly117.projetyls.com	projetyls.com	Informational	Élevé
wsly163.projetyls.com	projetyls.com	Informational	Élevé
wsly125.projetyls.com	projetyls.com	Informational	Moyen
alamotte_iPhone XS Max	AAD joined	Informational	Moyen
vmy026.projetyls.com	projetyls.com	No known ris...	Moyen
vmy027.projetyls.com	projetyls.com	No known ris...	Moyen
az-admin01.projetyls.com	projetyls.com	No known ris...	Moyen
azly-001	Workgroup	No known ris...	Moyen
az-ad01.projetyls.com	projetyls.com	No known ris...	Moyen
wsly164	AAD joined	No known ris...	Élevé
wsly187.projetyls.com	projetyls.com	No known ris...	Moyen
wsly185.projetyls.com	projetyls.com	No known ris...	Moyen

### Liste des alertes

Alertes									
En janvier, nous avons annoncé la dépréciation de l'API SIEM MDE le 1er mars dans un billet du Centre de messages (MC31104). Pour les clients qui utilisent toujours cette API, nous avons automatiquement étendu le support jusqu'au 1er avril. Reportez-vous à Dépréciation de l'API SIEM héritée - Microsoft Tech Community pour obtenir des conseils sur le passage à d'autres API et correctifs SIEM. Si vous avez besoin d'aide pour la migration, contactez le support.									
Voir le Centre de conformité Microsoft 365 pour des fonctionnalités supplémentaires liées à la conformité									
↓ Exporter 1 semaine Gérer les alertes Personnaliser les colonnes Filtrer									
Nom de l'alerte	Balises	Gravité	État de l'examen	État	Catégorie	Source de détection	Ressources affectées	Première activité	Dernière activité ↓
TEST_Brute-force		Faible	Type d'alerte non prise...	Nouveau	Activité suspecte	Microsoft Defender for...	Active Directory	27 mars 2022 20:18	27 mars 2022 20:18
TEST_Brute-force		Faible	Type d'alerte non prise...	Nouveau	Activité suspecte	Microsoft Defender for...	Active Directory	27 mars 2022 16:28	27 mars 2022 16:28
Délégation BAL		Élevé	Queue'd	Nouveau	Autorisations	MOO	NT AUTHORITY\SY...	27 mars 2022 10:00	27 mars 2022 10:04
TEST_Brute-force		Faible	Type d'alerte non prise...	Nouveau	Activité suspecte	Microsoft Defender for...	Active Directory	27 mars 2022 08:14	27 mars 2022 08:14
TEST_Brute-force		Faible	Type d'alerte non prise...	Nouveau	Activité suspecte	Microsoft Defender for...	Active Directory	27 mars 2022 00:12	27 mars 2022 00:12

### Liste des incidents

Incidents										
Incidents et alertes les plus récents										
Rechercher un nom ou ... Filtrer Personnaliser les colonnes 1 Week										
Filtres: État: Nouveau +1 Gravité: Élevé +2										
nom de l'incident	ID d'incid...	Balises	Gravité	État de l'examen	Catégories	Ressources affectées	Alertes actives	Service Sources	Detection Sources	Première activité
TEST_Brute-force	1053		Low	1 État de l'enquête	SuspiciousActivity	Active Directory	1/1	Microsoft Defender...	Microsoft Defender...	27 mars 2022 20:18
TEST_Brute-force	1052		Low	1 État de l'enquête	SuspiciousActivity	Active Directory	1/1	Microsoft Defender...	Microsoft Defender...	27 mars 2022 16:28
TEST_Brute-force	1051		Low	1 État de l'enquête	SuspiciousActivity	Active Directory	1/1	Microsoft Defender...	Microsoft Defender...	27 mars 2022 08:14
TEST_Brute-force	1050		Low	1 État de l'enquête	SuspiciousActivity	Active Directory	1/1	Microsoft Defender...	Microsoft Defender...	27 mars 2022 00:12



# Check Phishing/Malware

## MORNING CHECK

### Malware

The screenshot shows the 'Explorateur' interface for malware detection. It includes a search bar with filters for date and time, and a main area displaying 'Aucune donnée à afficher' (No data to display) twice, indicating that no malware was detected in the selected content.

### Phishing

The screenshot shows the 'Phishing' interface. It features a bar chart titled 'Action de distribution' showing the number of messages placed in the spam folder (blue) or blocked (purple) over time. Below the chart is a table of messages with columns for date, subject, recipient, status, sender, and actions.

Date (UTC +02:00)	Objet	Destinataire	Balises	Expéditeur	Actions suppl.	Emplacement ...	Lieu de livrai...
28 mars 2022 08:00	Fermeture exceptionnelle pour inventaire	jnovi@projetlys.com	-			Dossier de co...	Dossier de co...
28 mars 2022 07:36	Profitez de nos offres spéciales pro	dancian@projetlys.com	-			Quarantaine	Quarantaine
28 mars 2022 05:07	Vous risquez de perdre votre prochain budg	contact@projetlys.com	-			Dossier de co...	Dossier de co...
28 mars 2022 05:02	Vous risquez de perdre votre prochain budg	contact@projetlys.com	-			Dossier de co...	Dossier de co...
28 mars 2022 04:43	Vous risquez de perdre votre prochain budg	contact@projetlys.com	-			Dossier de co...	Dossier de co...
28 mars 2022 04:24	Vous risquez de perdre votre prochain budg	contact@projetlys.com	-			Dossier de co...	Dossier de co...
28 mars 2022 01:53	If you can't have sex when you want somethi	contact@projetlys.com	-			Quarantaine	Quarantaine

# Utilisateurs à risque Azure & Rapport MS Identity

## MORNING CHECK

Utilisateurs à risque

En savoir plus | Télécharger | Sélectionner tout | Confirmer que le ou les utilisateurs sont compromis | Ignorer le risque de l'utilisateur ou des utilisateurs | Actualiser | Colonnes | Des commentaires ?

Actualisation automatique : Désactivé | Afficher les dates au format : Local | Niveau de risque : Bas, Moyen, Haute | Ajouter des filtres

<input type="checkbox"/> Utilisateur ↑↓	État à risque ↑↓	Niveau de risque ↑↓	Dernière mise à jour du risque ↑↓
<input type="checkbox"/> Alexa	À risque	Moyen	26/03/2022, 15:27:01
<input type="checkbox"/> Enor	À risque	Bas	25/03/2022, 11:17:43

### Lateral movements paths to sensitive accounts

Daily "Lateral movements paths to sensitive accounts" report in [projetlys: 3/27/2022](#)

No lateral movement paths were found.

[Manage notification settings](#)

### Password exposed in cleartext

Daily "Passwords exposed in cleartext" report in [projetlys: 3/27/2022](#)

There were no LDAP authentications which exposed user passwords in cleartext during the requested time period.

[Manage notification settings](#)

### Summary

Daily "Summary" report in [projetlys: 3/27/2022](#)

There was no relevant data to generate a report during the requested time period.

[Manage notification settings](#)

### Modification to sensitive groups

Daily "Modifications to sensitive groups" report in [projetlys: 3/27/2022](#)

There were no sensitive group membership modifications during the requested time period.

[Manage notification settings](#)

# 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

The screenshot shows the Microsoft Defender for Identity console interface. The top navigation bar includes the Microsoft logo, the text 'Microsoft Defender for Identity | projetlys | Chronologie', and a search bar 'Rechercher parmi les utilisateurs'. Below the navigation bar, there is a blue banner with the text 'Nouvelle expérience d'investigation disponible. Essayer'. The main content area displays a timeline of security events. On the left, there is a filter sidebar with the following items: 'Toutes [2]', 'Haute(s) [1]', 'Moyenne(s) [1]', 'Basse(s) [0]', 'Ouverte(s) [0]', 'Clôturée(s) [2]', and 'Supprimée(s) [0]'. The timeline shows two events: 1. At 00:03 on 2 dec. 2021, a yellow event titled 'Reconnaissance du principal de sécurité (LDAP)' with the description 'Un acteur sur VMLY016 a envoyé une requête LDAP suspecte à SRVDC02, recherchant 3 types d'énumération dans projetlys.com'. 2. At 12:33 on 1 dec. 2021, a red event titled 'Suspicion d'attaque DCSync (réplication de services d'annuaire)' with the description 'MSOL\_58d386a0e20f sur VMLY030 a envoyé 68 demandes de réplication à 2 contrôleurs de domaine.'.

# Résumé quotidien & Alertes

## MORNING CHECK

### 8. Résumé du jour

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

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

### 9. Alerte en cours

RCA : [Alerte en cours d'investigation \(RCA\) docx](#)

Liste 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

# Questions ?

---





# Merci !

---

[www.bluesoft-group.com](http://www.bluesoft-group.com)

[www.projetlys.com](http://www.projetlys.com)

