

Protégez vos équipes *au bon moment*



Mantra

Real-time Cyber Awareness

Protégez vos utilisateurs *au bon moment*

Utilisateurs

>

Email

>

Navigateur



Approche préventive



Approche temps-réel



Cyber
Awareness



Phishing
Simulation



Smart
Banners



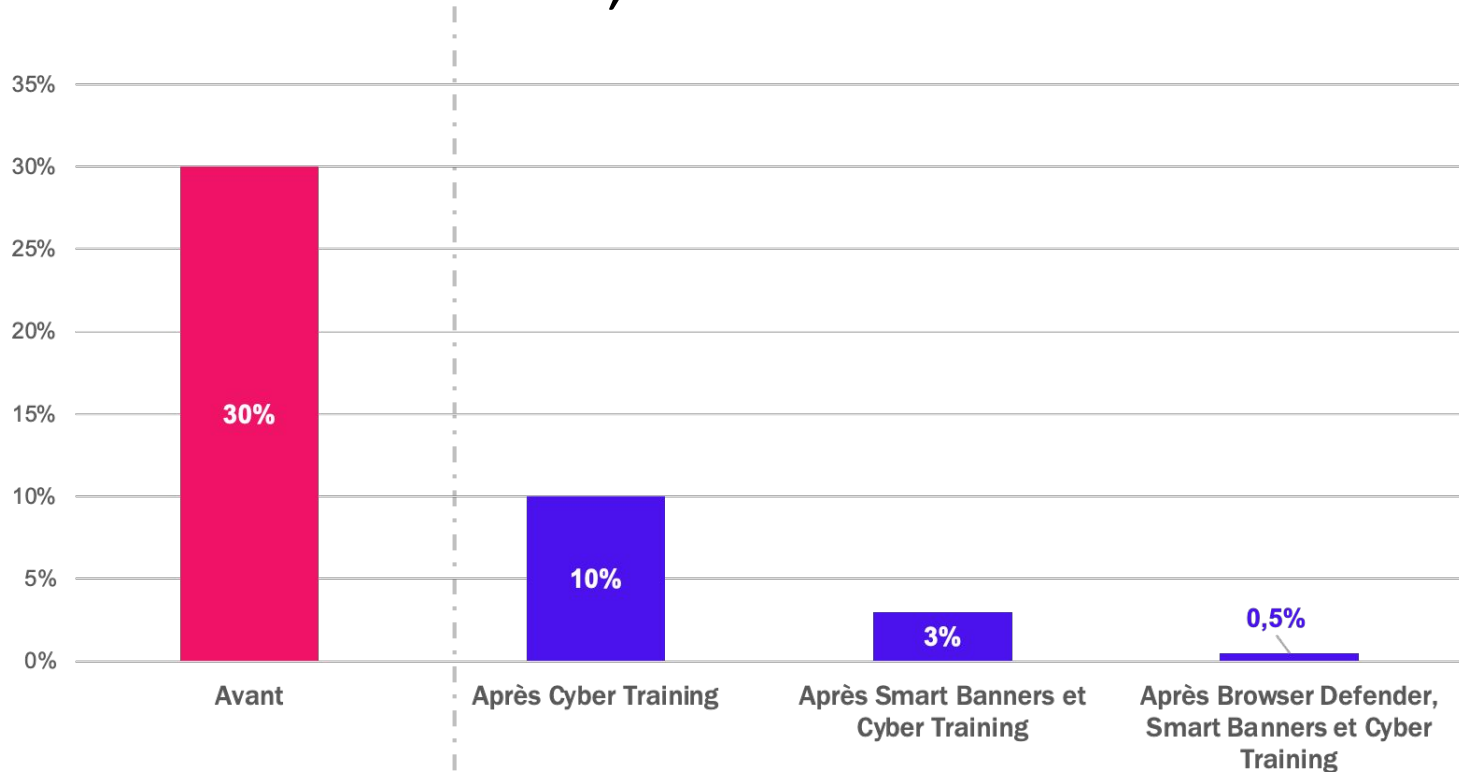
Browser
Defender



Mantra

Real-time Cyber Awareness

Réduire le taux de compromission de vos collaborateurs vers 0,5 %



Formez vos collaborateurs à la cybersécurité

ONBOARDING TRACK

?

Pourquoi la cybersécurité est-elle importante ?

A COMPLETER

Cette introduction explique pourquoi le risque cyber constitue plus que jamais une menace pour les entreprises et donne quelques exemples d'attaques qui ont eu lieu sur des entreprises françaises.

Cours Master

Progress

Completed

RUN MODE

?

Qu'est-ce que le phishing ?

A COMPLETER

L'objectif de ce cours est de déterminer les éléments caractéristiques du phishing pour comprendre concrètement ce que c'est.

Cours Master

Progress

Completed

?

Comment détecter une attaque de phishing ?

A COMPLETER

Cette leçon fournit les principaux éléments qui peuvent permettre d'identifier une attaque de phishing.

Cours Master

Progress

Completed

?

Quels moyens utilisent les hackers pour attaquer ? (cloned)

A COMPLETER

Ce module donne des moyens fréquemment utilisés par les cybercriminels pour mener une attaque.

Cours personnalisé - Définir les changements pour assigner le cours

Progress

Completed

?

Qui sont les hackers et quelles sont leurs motivations ?

EN COURS

Le but de ce module est de présenter les différents profils de hackers qui existent, d'expliquer leurs motivations et leurs modes opératoires.

Cours Master

Progress

Completed

Users Progress

Display subscribed courses only

Add filter

First name	Last name	Language	Departments	Completion ↑	Status	?	POURQUOI LA C...	WHY AM I A TA...	QU'EST-CE QUE...	WHO ARE HACKE...	QUELLES SONT L...	HOW TO DETECT...	QUEST-CE QUE...	QUEST-CE QUE...	COMMENT LE PH...
Nikeisha	Allen	FR	Sales	82%	On Track		✓	✓	✓	✓	✓	✓	✓	✓	✓
Willow	Evans	FR	Tech	40%	On Track		✓	✓	...	...	...	✓	✓	✓	...
Lyndsey	Campbell	EN	RH	27%	On Track		✓	✓	...	...	...	✓	✓	...	...

14:01

◀ LinkedIn

Alex >

Disponible

completé votre module de cybersécurité (5 min. max)

⌚

4

✗ Dommage, la bonne réponse était le phishing

Quel canal les cybercriminels utilisent pour faire du phishing ?

☎ Seulement les appels

✉ Uniquement le mail

📱 Uniquement les SMS

Tous ces canaux

Tous ces canaux

✓ Bravo c'est la bonne réponse

Les cybercriminels sont susceptibles d'utiliser tous ces canaux

+ Taped un message

😊

➡

+ Create course

+ Create course with AI

⌕

Principales fonctionnalités

- Base de 25 tutoriels & 1 nouveau tutoriel tous les mois ✓
- Approche conversationnelle ✓
- Système de relance automatique et manuelle ✓
- Contenu des tutoriels 100% éditable ✓
- Suivi avancement via tableaux de bord ✓

Mantra

Formez vos collaborateurs à la cybersécurité

Liste des leçons disponibles

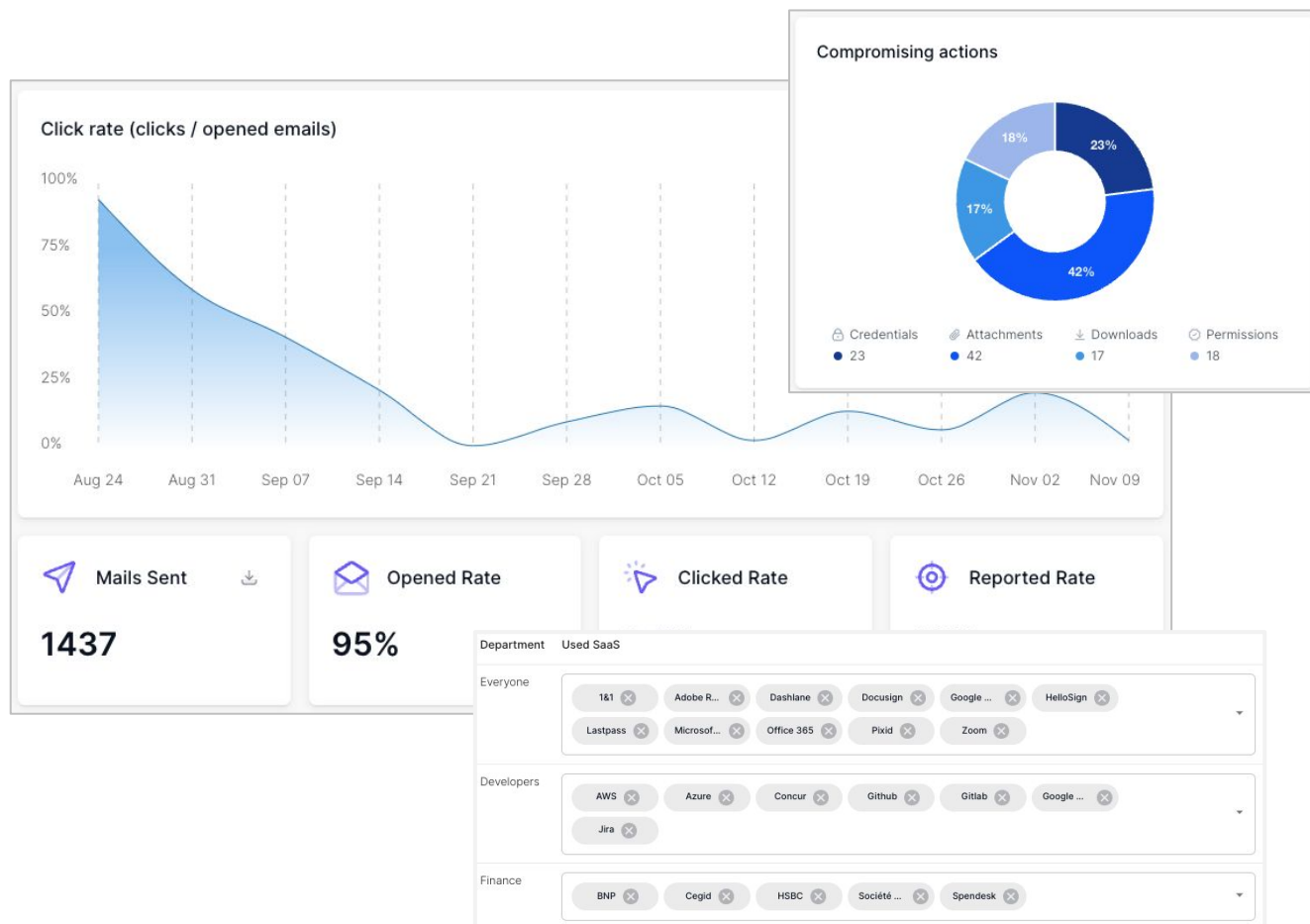
1. Pourquoi la cybersécurité est-elle importante ?
2. Qu'est-ce que le spear-phishing ?
3. Comment réagir si je suis victime d'une attaque ?
4. Qu'est-ce qu'une fuite de données ?
5. Pourquoi suis-je la cible des hackers ?
6. Quelles sont les principales méthodes de phishing ?
7. Le Phishing sur LinkedIn : Apprendre à le détecter
8. Les bonnes pratiques des mots de passe
9. Comment éviter une arnaque sur votre compte en banque personnel?
10. Configurer la réponse automatique de sa boîte mail
11. Qu'est-ce que le Shadow-IT ?
12. Qu'est-ce que le RGPD ?
13. Empreinte numérique et bonnes pratiques
14. Comment le phishing par téléphone fonctionne-t-il ?
15. Comment réduire les risques cyber en télétravail ?
16. Quels moyens utilisent les hackers pour attaquer ?
17. Pourquoi la sécurité physique est importante pour la cybersécurité ?
18. Comment le Wi-Fi peut être dangereux ?
19. Pourquoi les attaques par ransomware sont si dangereuses ?
20. Qu'est-ce que la fraude au président ?
21. Comment détecter une attaque de phishing ?
22. Qui sont les hackers et quelles sont leurs motivations ?
23. Les attaques via Microsoft Teams
24. Le phishing via QR Code
25. ChatGPT & autres : comment utiliser les IA en toute sécurité ?



Principales fonctionnalités

- Ciblage des tutoriels par groupe de personnes ✓
- Approche gamifiée ✓
- Evaluation à la fin de chaque tutoriel (quizz de validation) ✓
- Intégrations Teams et Slack ✓
- Intégration LLM ✓

Entraînez vos utilisateurs en situation réelle

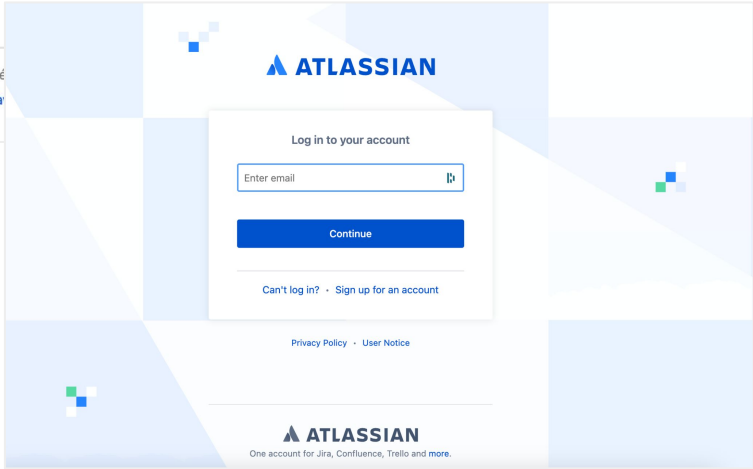
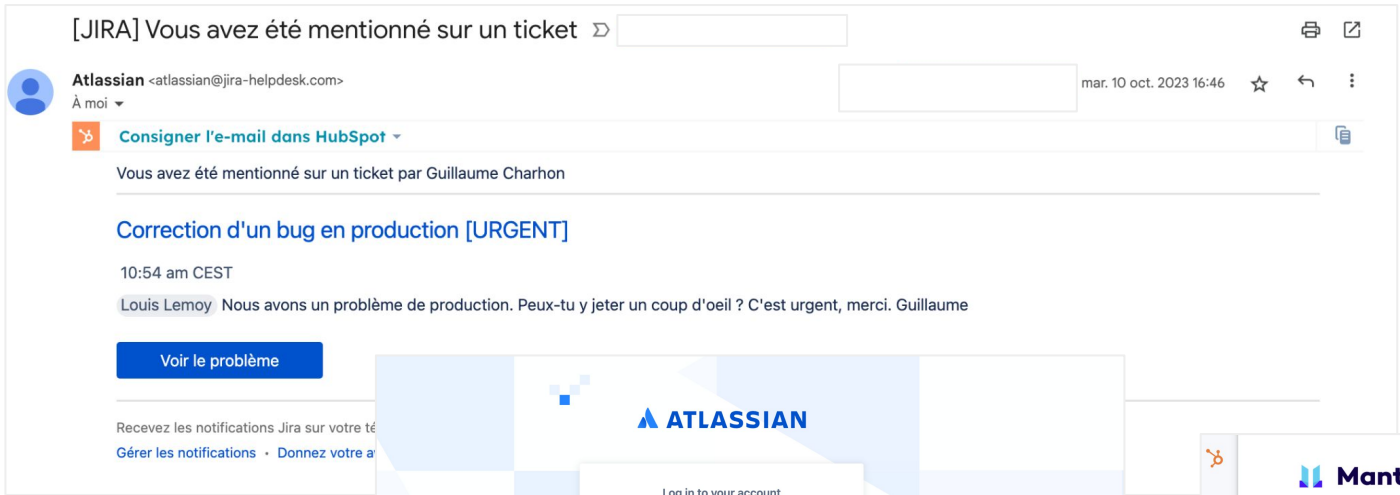


Principales fonctionnalités

- Base de 500 templates ✓
- Simulation d'attaques de spear-phishing ✓
- Parcours gamifié ✓
- Solution 100% automatisée ✓
- Synchronisation annuelle Google Workspace / O365 ✓
- Campagnes sur-mesure ✓

Entraînez vos utilisateurs en situation réelle

Exemple d'une attaque de spear phishing



Spear-phishing

- Effet d'urgence
- Near Domain
- Usurpation DSI
- Ciblage par département

Protégez vos utilisateurs *au bon moment*

Utilisateurs

>

Email

>

Navigateur



Approche préventive

Approche temps-réel



Cyber
Awareness



Phishing
Simulation



Smart
Banners



Browser
Defender



Mantra

Real-time Cyber Awareness

Aidez vos utilisateurs à détecter les vraies attaques avec l'IA

/AVANT

27 personnes remarquent votre profil

ExternalInboxBanners - FR/Banners - Without

View Linked's ProfileNov 9, 2022, 10:53 AM

FrenchEnglishTranslate messageTurn off for: FrenchSave email as template

LinkedIn

Votre profil est sous son meilleur jour

Votre travail et vos réalisations ne passent pas inaperçus

27

vues du profil

Voir qui regarde

Cet e-mail est destiné à Pierre Ribault. Découvrez pourquoi nous précisons ceci.

Vous recevez des e-mails de Résumé Identité professionnelle.

Se désinscrireAide

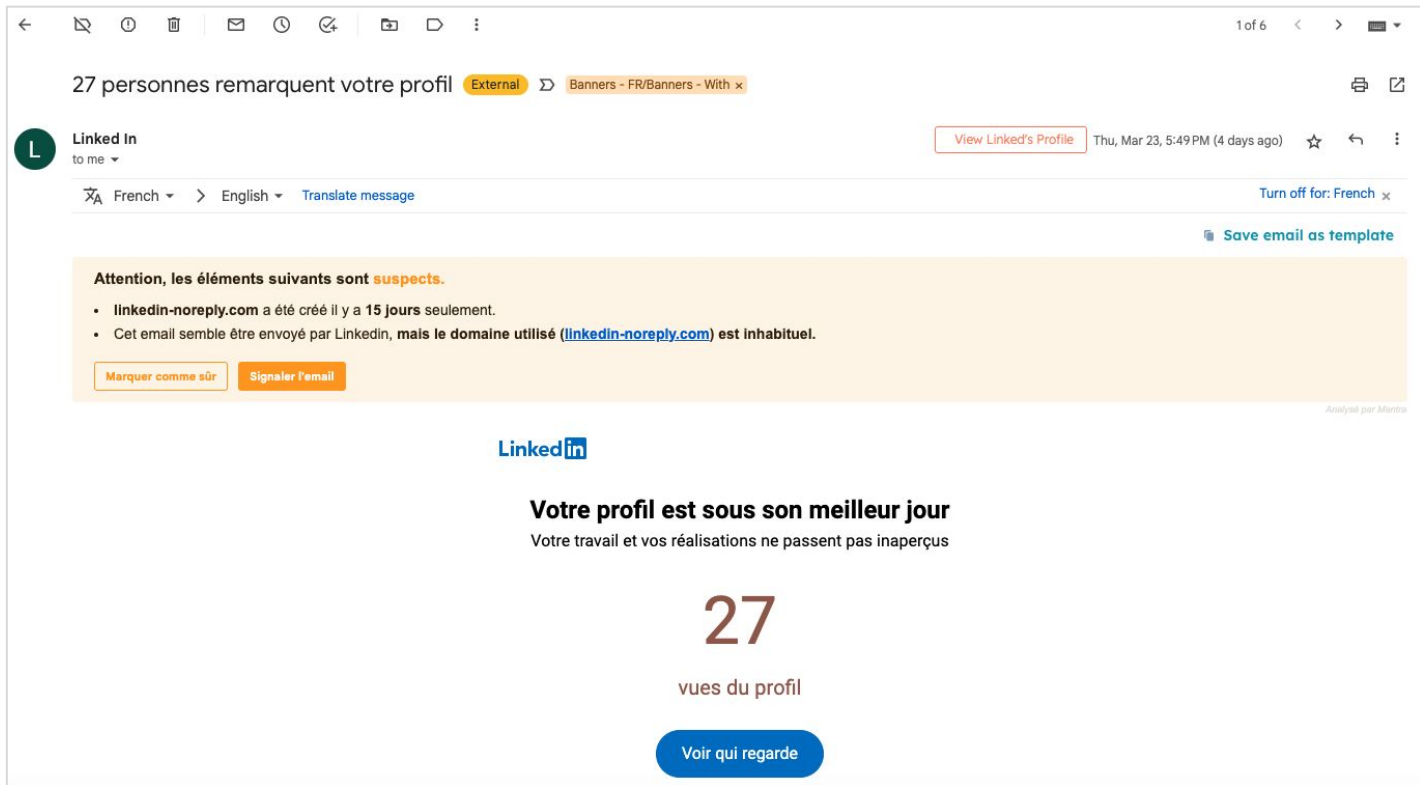
Attack types

All Phishing

Attachment Phishing

Aidez vos utilisateurs à détecter les vraies attaques avec l'IA

/APRES

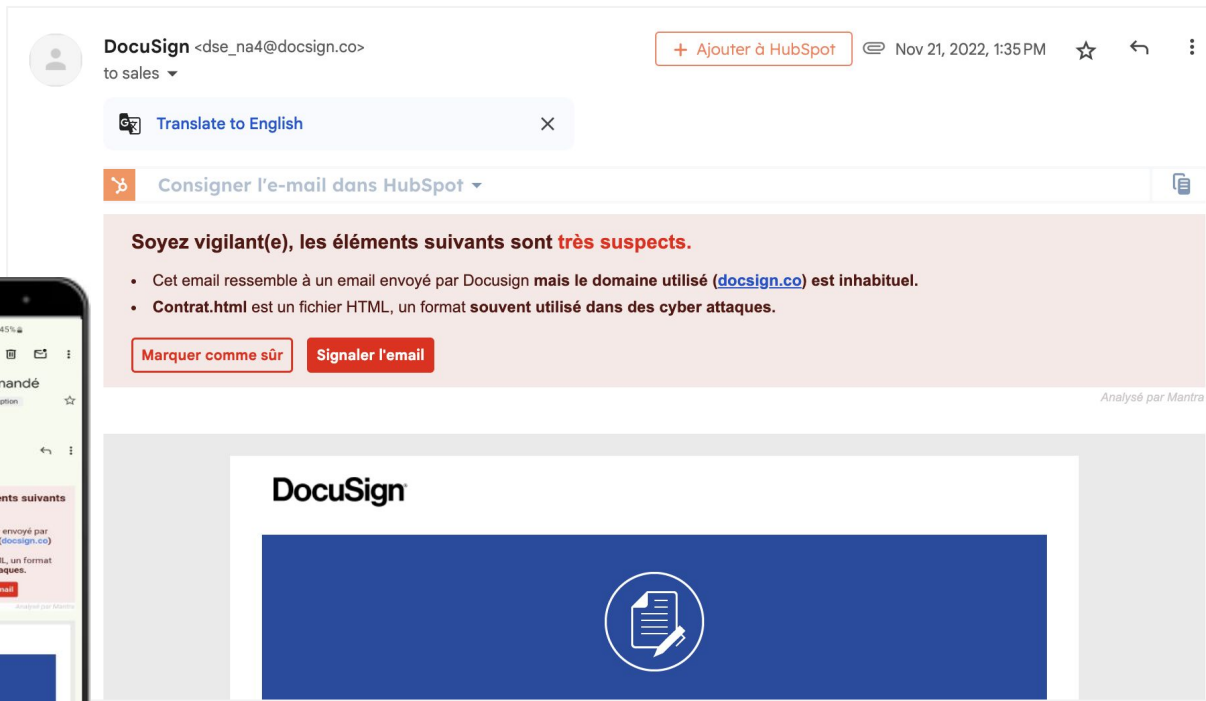


Attack types

- All Phishing ✓
- Attachment Phishing ✓
- > 40 data points analyzed ✓
- 2 click deployment ✓
- All devices ✓

Aidez vos utilisateurs à détecter les vraies attaques avec l'IA

/APRES



🔗 Attack types

- All Phishing ✓
- Attachment Phishing ✓
- > 40 data points analyzed ✓
- 2 click deployment ✓
- All devices ✓

Exemple de contrôle des points de métadonnées

/Non Exhaustive

Data Point

Category

Newly Created Domain

Domain

Bulk Registered Domain

Domain

Internal Contact Near Domain

Domain, Graph

Different Reply-To

Sender

Dangerous Extension (LNK, ISO, etc.)

Attachment

Suspicious Extension (HTM, ZIP)

Attachment

Public Cloud Link

Link

No-Domain Related Link

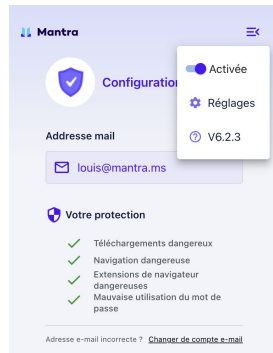
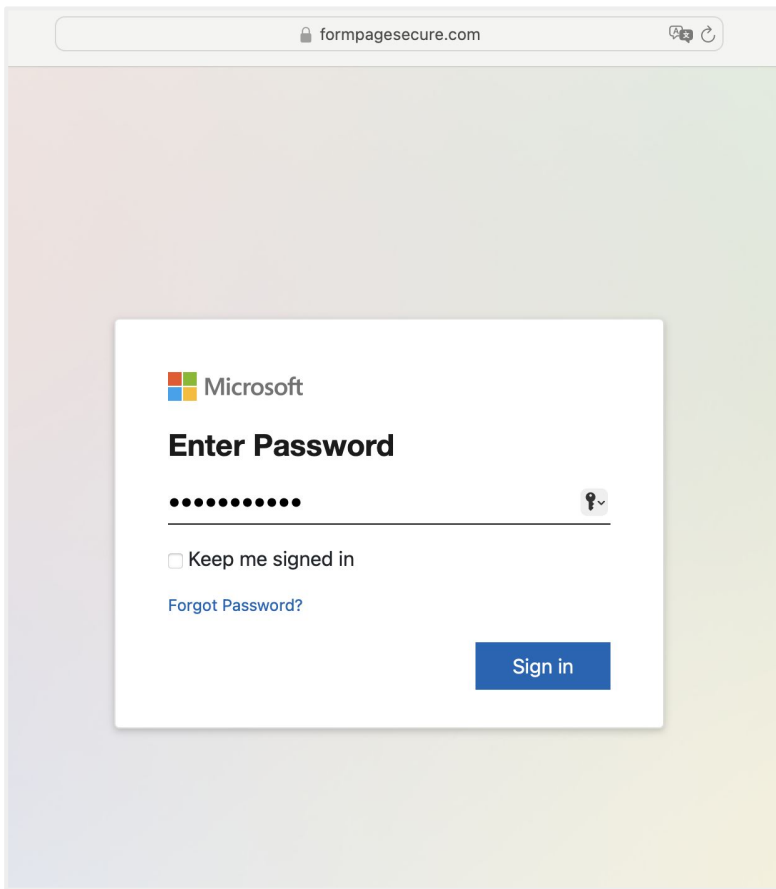
Link

First Time Sender

Graph

Empêchez la compromission des comptes utilisateurs

/AVANT

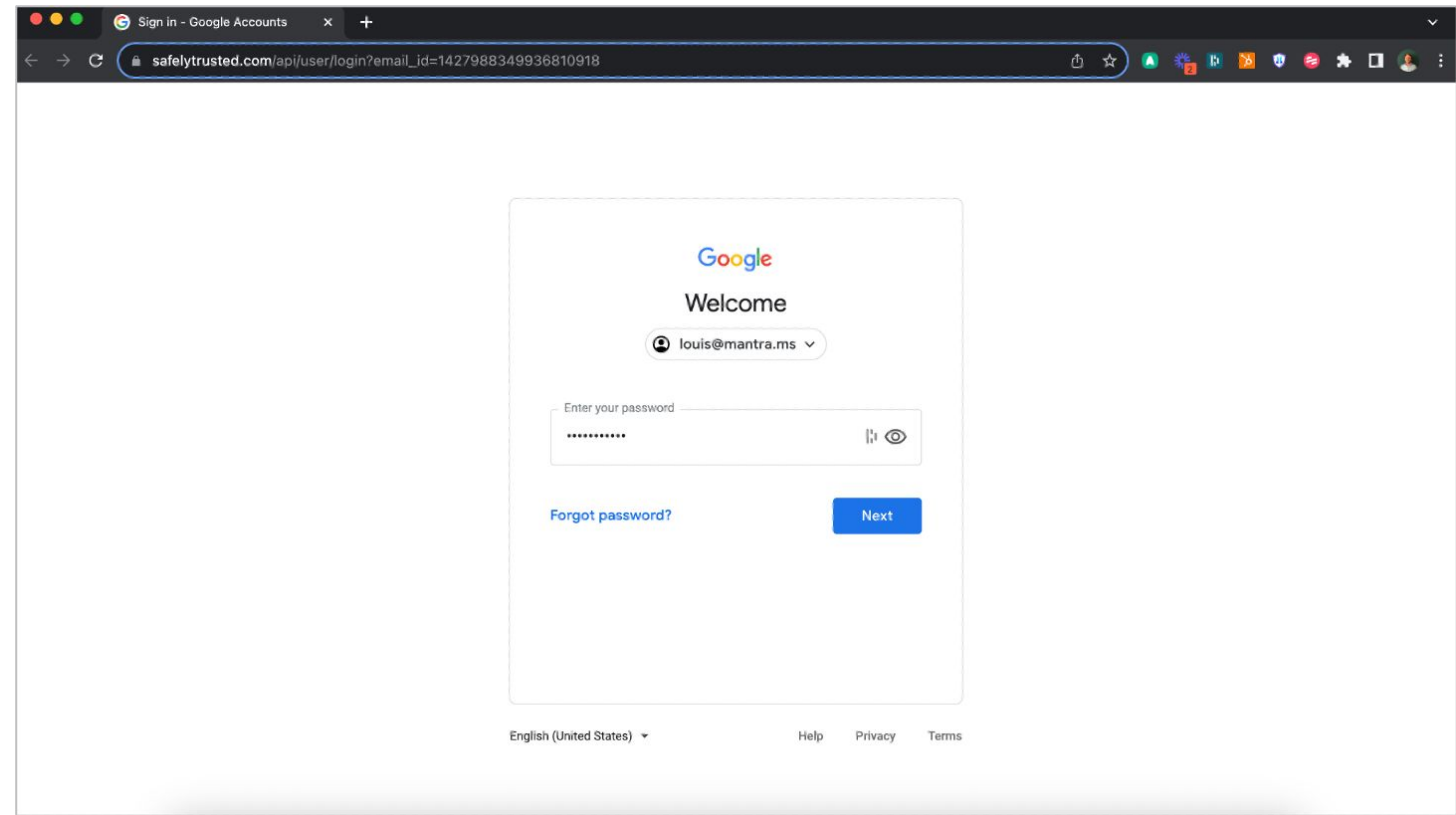


Attack Types

- Credential Phishing ✓
- Download Phishing ✓
- Extension Monitoring ✓

Empêchez la compromission des comptes utilisateurs

/AVANT



Attack Types

- Credential Phishing ✓
- Download Phishing ✓
- Extension Monitoring ✓

Empêchez la compromission des comptes utilisateurs

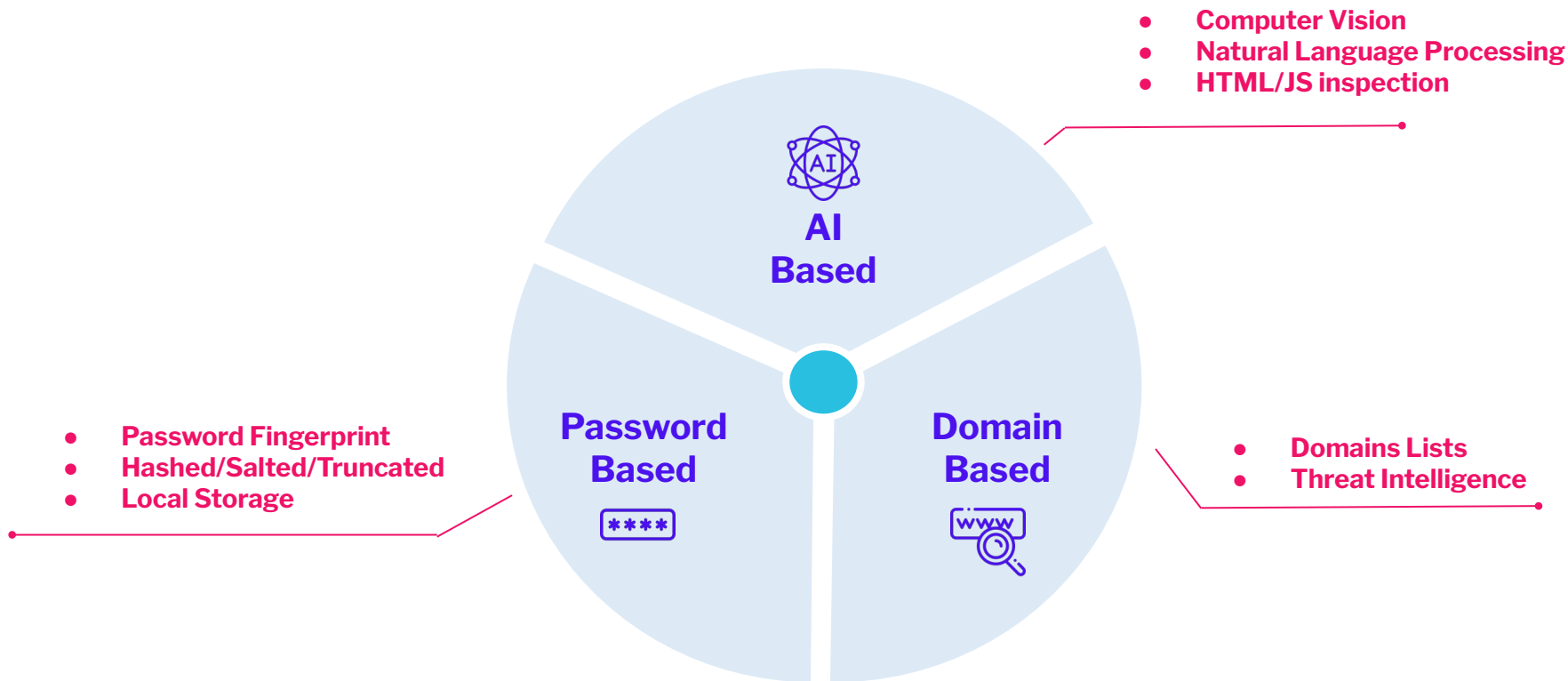
/APRÈS

The screenshot shows the Mantra Browser Defender interface. At the top, there's a header with the Mantra logo. Below it, a large blue circle with a white exclamation mark icon is next to the title 'Utilisation anormale de votre mot de passe'. Underneath, the domain 'safebrowsingpage.com' is listed. A section titled 'Pourquoi cette page s'affiche-t-elle ?' contains two bullet points: 'Vous êtes sur le point d'utiliser votre mot de passe professionnel sur un site tiers.' and 'Deux cas sont possibles :'. The second bullet point has two sub-points: 'Cas n°1 : il peut s'agir d'une attaque cyber ayant pour but de voler vos identifiants.' and 'Cas n°2 : c'est un site légitime qui pourrait être piraté et votre mot de passe serait récupéré par un hacker.' Below this, a section titled 'Que dois-je faire ?' contains one bullet point: 'Nous vous recommandons de changer le mot de passe de votre compte professionnel.' At the bottom, there are two buttons: 'Ignorer une fois' and 'Ignorer toutes les alertes sur ce domaine'. The footer contains the text 'Pour toute demande, contactez dev-extension@mantra.ms'.

Attack Types

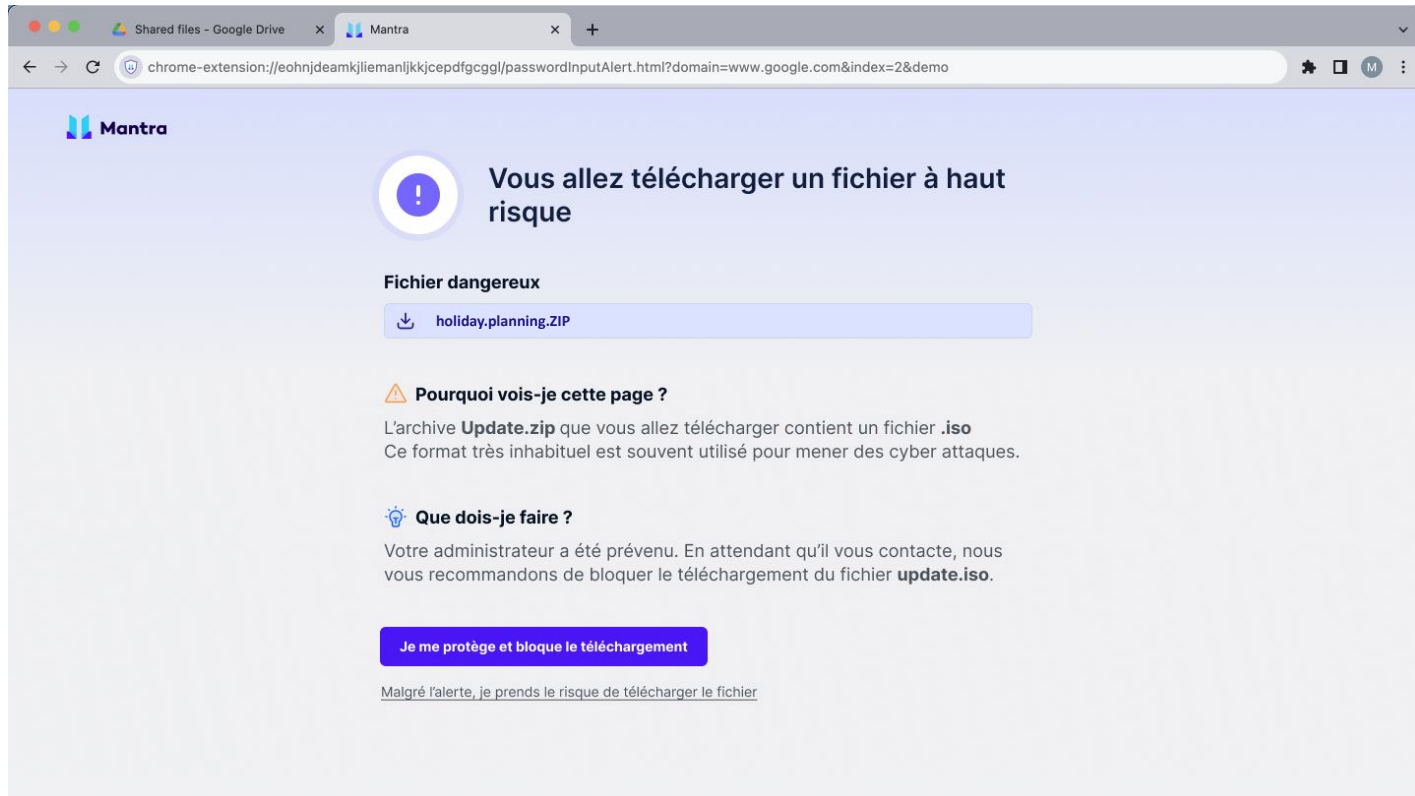
- Credential Phishing ✓
- Download Phishing ✓
- Extension Monitoring ✓

Le Browser Defender utilise 3 méthodes complémentaires



Protégez vos collaborateurs de téléchargements à risque

/AFTER



Shared files - Google Drive x Mantra x +

chrome-extension://eohnjdeamkjiemanljkkjcepdfgpggl/passwordInputAlert.html?domain=www.google.com&index=2&demo

Mantra

Vous allez télécharger un fichier à haut risque

Fichier dangereux

📄 holiday.planning.ZIP

Pourquoi vois-je cette page ?

L'archive **Update.zip** que vous allez télécharger contient un fichier **.iso**.
Ce format très inhabituel est souvent utilisé pour mener des cyber attaques.

Que dois-je faire ?

Votre administrateur a été prévenu. En attendant qu'il vous contacte, nous vous recommandons de bloquer le téléchargement du fichier **update.iso**.

Je me protège et bloque le téléchargement

Malgré l'alerte, je prends le risque de télécharger le fichier

Attack Types

- Credential Phishing ✓
- Download Phishing ✓
- Extension Monitoring ✓

Pilotez les actions compromettantes de vos collaborateurs

Browser Defender Dashboard

Timeframe
1 Week

Users with active extensions

500

Awaiting login: 40
Disabled by user: 1
Inactive (> 30 days): 3

Password misuse alerts

27

With domain set as trusted: 16

Dangerous download alerts

21

With file downloaded: 6

Dangerous browsing alerts

17

With page visited: 5

Password Strength Distribution

Strong: 182 users

Average: 114 users

Weak: 160 users

Data per User

Search

Sort

Firstname	Lastname	Email	Language	Departments	Status	Version	Events
Callan	Myers	callan@acme.com	fr		Awaiting login	1.0.0	4 4 5
Bibiana	Williams	bibiana@acme.com	fr		Protected	1.0.0	5 4 3

Extension governance

Search

Sort

ALL

Name	Users	Permissions
Dashlane — Passwo...	4	Intrusive
Google Docs Offline	3	Minimally
Fidget Spinner	1	Moderate
In house extension	1	Intrusive

Rows per page: 8 1-4 of 4

In house extension

Extension developed by Lyndsey

Permissions Intrusive

This extension requires the following permissions:
read and change all data on websites

User details

Email	Version	Install mode	Status	Last detected
lyndsey@acme.com	0.0.1	Development	✓	19-11-2023 12:11

Rows per page: 5 1-1 of 1

Password Misuse

Timeframe
1 Year

Event Distribution

Event Logs

Search

Sort

Time (UTC)	Email	Domain	User action	Domain action	Remediation
15-09-2023 15:55	lyndsey@acme.com	not-risky-domain.io	Domain set as trusted	Block None Trust	
14-09-2023 10:35	matt@acme.com	[ghub:3767:domain-update.xyz]	Warning ignored once	Block None Trust	

- Password reuse/weak* ✓
- Credential Phishing ✓
- Download Phishing ✓
- Extension Monitoring ✓

Ils nous font confiance



ARTEFACT



SeLogger



ERIC BOMPARD



Dispositif d'accompagnement

Semaine 1



Kickoff



Formulaire technique



Setup technique (1/2)

Semaine 2



Audit de phishing (*)



Restitution des résultats (*)

Semaine 3



Setup technique (2/2)



Formation & transfert
de compétences



Elaboration du Plan
de communication



Lancement du programme
Mantra

Tout le long du programme : Accompagnement et suivi en continu par l'équipe Customer Success de Mantra

Accompagnement continu pour garantir le succès du programme

RUN



Attribution d'un Chef
de Projet Cyber



Réalisation de Business
Review

(*) Optionnel

A propos de Mantra

1. Equipe



Créé en 2019



Basé sur la tech.

**Guillaume
Charhon**



CTO

15 ans d'expérience
Chef d'équipe technique pour 30 personnes

**Gaspard
Droz**



CEO

10 ans d'expérience
Ancien consultant en stratégie et IT

2. Investisseurs & partenaires

VCs

bpifrance axeleo oneRagtime

**Xavier
Perret**



Microsoft Azure
Directeur France

**Laurent
Hausermann**



VP Cyber
IoT Cisco
-
Co-fondateur Sentry.io

**Benjamin
Fabre**



Co-fondateur
Datadome

**Conseils & Business
Angels**

Roadmap



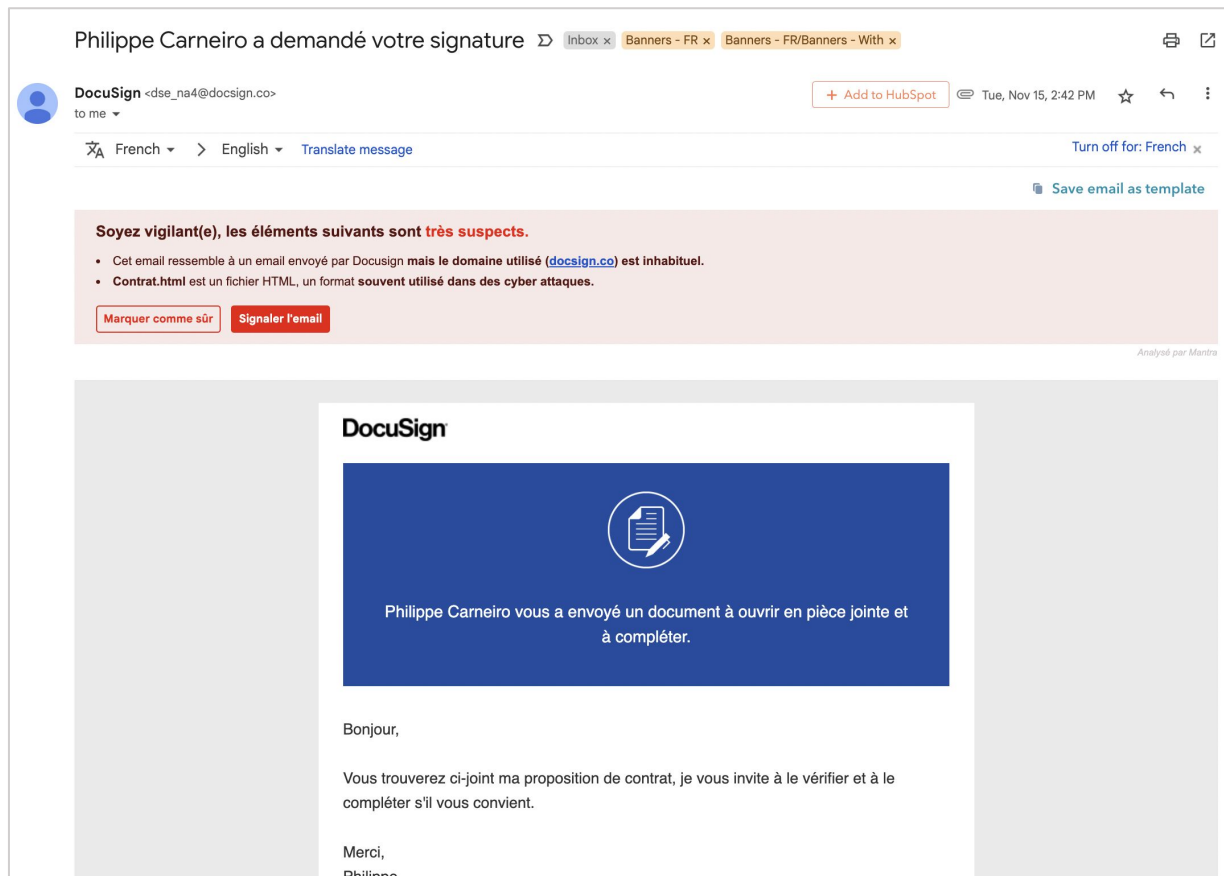
Nous prenons notre propre cybersécurité très au sérieux



Mantra est certifié SOC II Type 1

Real-time Cyber Awareness **Mantra**

Aidez vos utilisateurs à détecter les phishing



Détection d'une éventuelle usurpation d'identité

27 personnes remarquent votre profil

[Inbox](#) [Banners - FR](#) [Banners - FR/Banners - With](#)

LinkedIn <notification@linkedin-noreply.com>
to me

[View LinkedIn's Profile](#) Tue, Nov 15, 4:34 PM

[Turn off for: French](#)

[Save email as template](#)

Attention, les éléments suivants sont suspects.

- [linkedin-noreply.com](#) a été créé il y a 15 jours seulement.
- Cet email ressemble à un email envoyé par LinkedIn mais le domaine utilisé ([linkedin.com](#)) est inhabituel.

[Marquer comme sûr](#) [Signaler l'email](#)

Analysé par Mantra

LinkedIn

Votre profil est sous son meilleur jour
Votre travail et vos réalisations ne passent pas inaperçus

27
vues du profil

[Voir qui regarde](#)

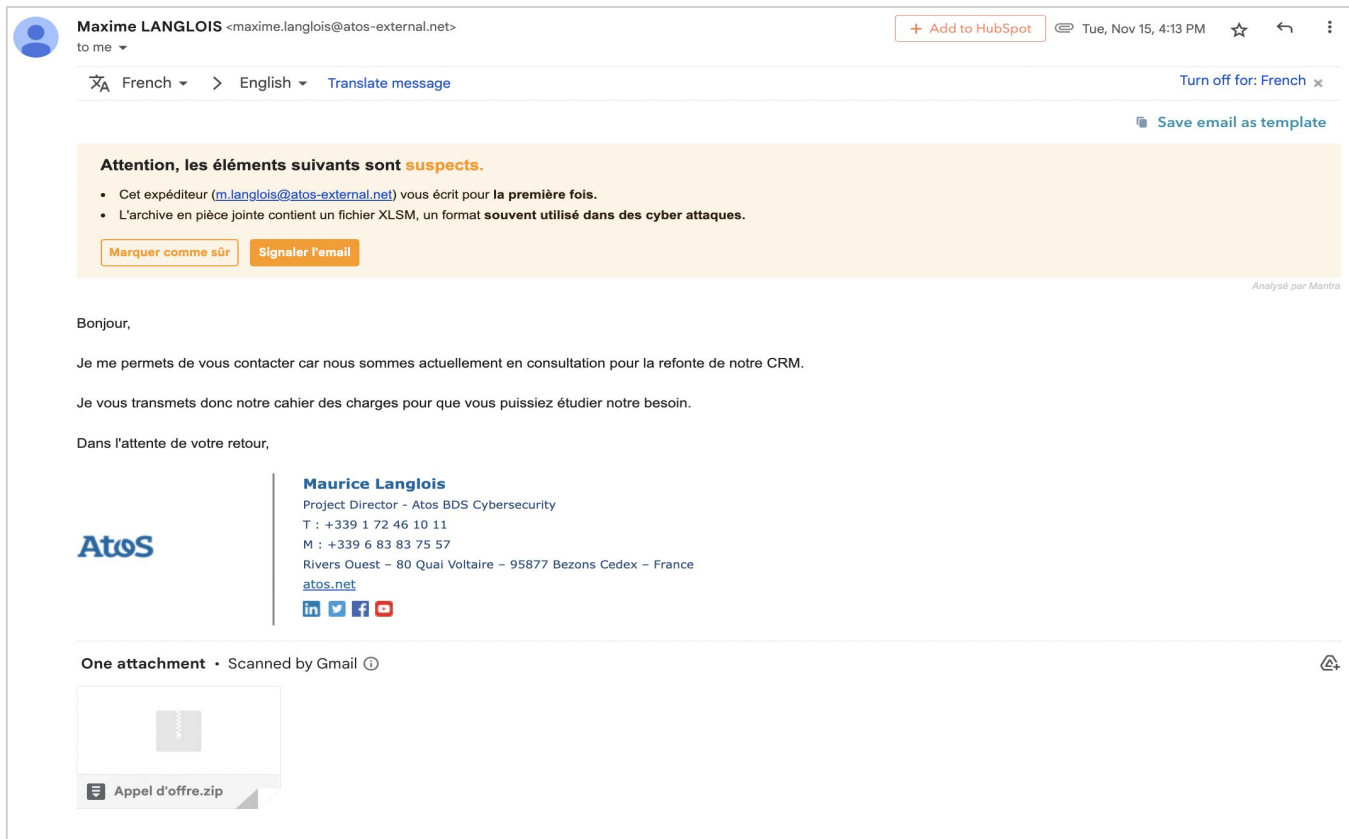


**Brand
Impersonation**



**Credentials
Attack**

Détectez des attaques potentielles par logiciels malveillants



**Brand
Impersonation**



**Suspicious
Attachment**

Détection de fraude financière

Changement compte de facturation

Exemple bannière mail

Laurent Chemla <laurent.chemla@elinoi.com>

À sales

+ Ajouter à HubSpot

lun. 21 nov. 13:36 (il y a 7 jours)

☆ ↶ ⋮

Enregistrer l'e-mail en tant que modèle

Soyez vigilant(e), les éléments suivants sont très suspects.

- Le nom de l'expéditeur est celui d'un contact mais l'adresse utilisée (laurent.chemla@elinoi.com) ne correspond pas à son adresse habituelle.
- Le contenu de l'email semble lié à des **éléments financiers**.
- C'est la **première fois** que cet expéditeur vous envoie un email.

Marquer comme sûr

Signaler l'email

Analyse par Mantra

Bonjour Gaspard,

Nous avons changé de banque, tu trouveras ci-joint notre nouveau RIB.

À partir de maintenant, pourriez-vous svp effectuer les futurs paiements sur ce compte?

Merci d'avance et à bientôt,

...

ÉLINOI

Laurent CHEMLA
Team Lead Account Manager @ Élinoi
laurent.chemla@elinoi.com
30 Rue Mogador 75009 Paris

1 pièce jointe • Analyse effectuée par Gmail

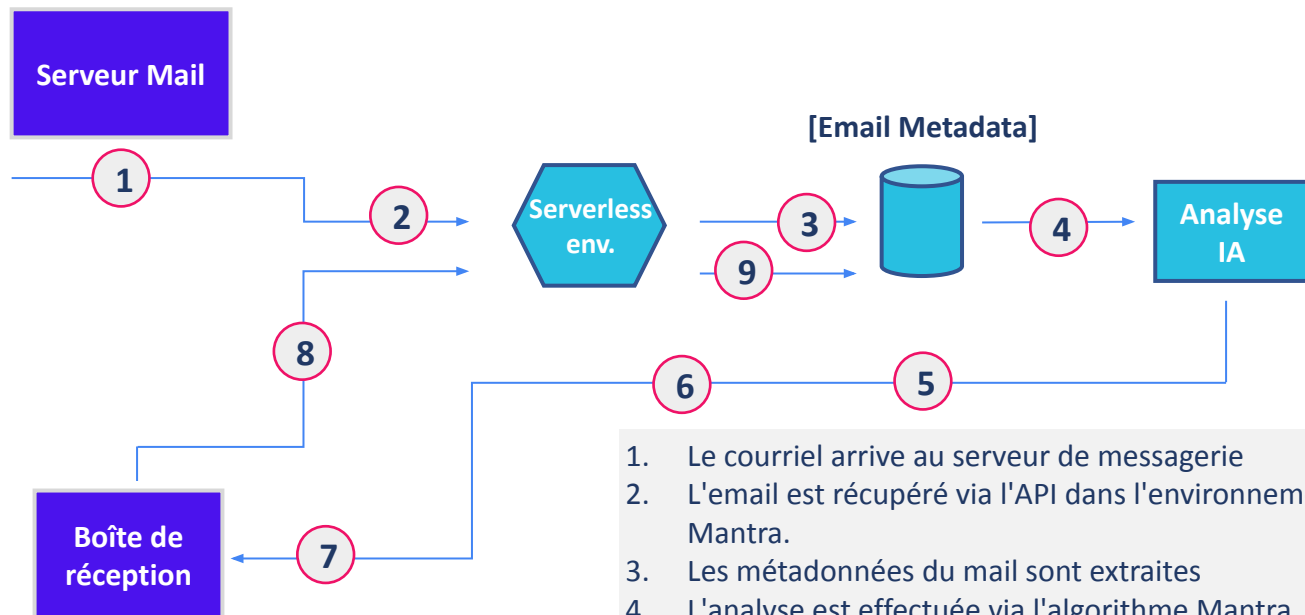
RIB.pdf

Contact
Impersonation

CEO
Fraud

 Mantra

Architecture & Flux



1. Le courriel arrive au serveur de messagerie
2. L'email est récupéré via l'API dans l'environnement sans serveur Sandbox de Mantra.
3. Les métadonnées du mail sont extraites
4. L'analyse est effectuée via l'algorithme Mantra.
5. Ajout de bannières (par copie ou modification)
6. Les informations DKIM/DMARC sont réécrites dans les en-têtes.
7. L'email est déplacé vers la boîte de réception
8. L'environnement temporaire Sandbox sans serveur contenant le contenu de l'e-mail est détruit.
9. Seules les méta-données hashées stockées sont conservées.