



La Région
Auvergne-Rhône-Alpes



SOMMETS DU TOURISME 2026

Atelier Session n°4



OpenSource Intelligence : ces données publiques qui parlent de vous !



Stéphane FONDJOU DOUNOU
Directeur Commercial et
Stratégie, OVIDE



Vincent DUSSEIRE
Directeur Technique et R&D
OVIDE



Lionel POINSOT
Directeur ENE – Experts du
Numérique en Entreprise

CAMPUS RÉGION^{ON} DU NUMÉRIQUE



CAMPUS CYBER AUVERGNE-RHONE-ALPES

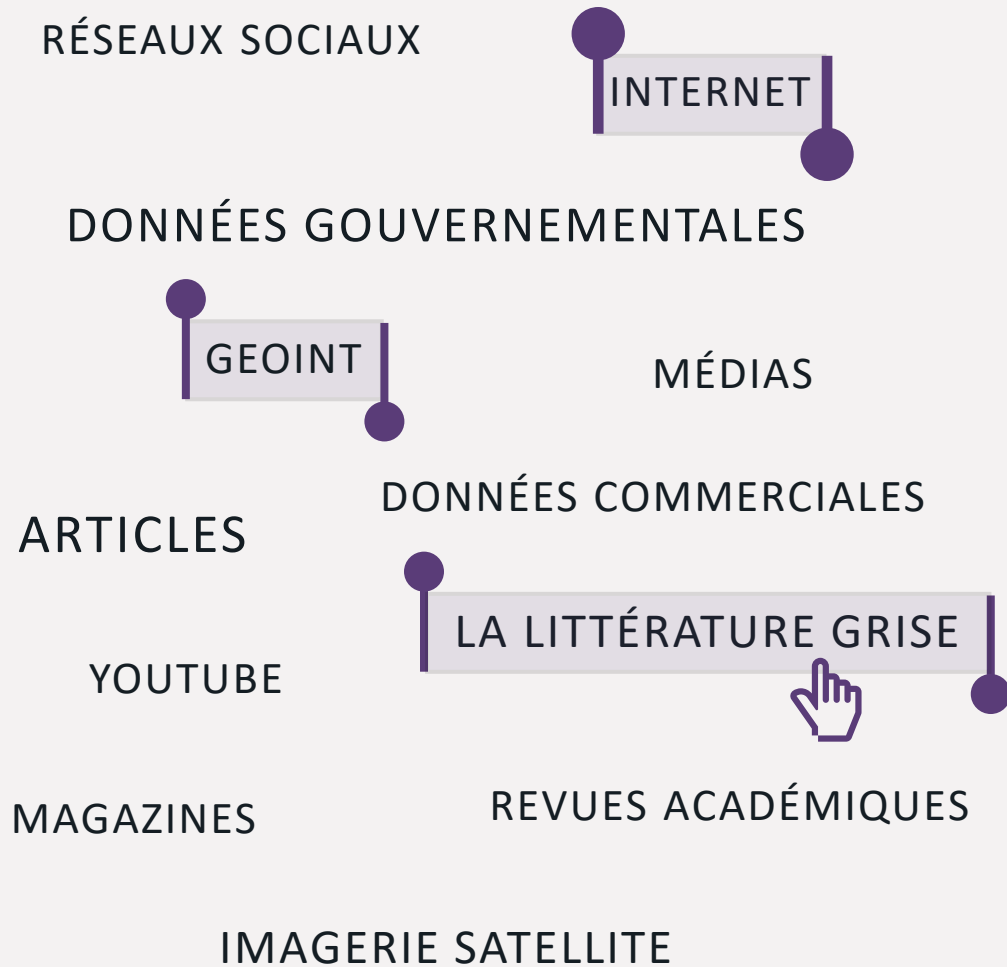
- ☐ Une stratégie
- ☐ Une gouvernance
- ☐ Des actions
- ☐ Un écosystème
- ☐ Un lieu totem
- ☐ Des évènements
- ☐ Des équipements
- ☐ Des résidents

DEMO

ovide

Formations ludiques en cybersécurité

OSINT : késako ?



(Acronyme de **Open Source IN**Telligence)

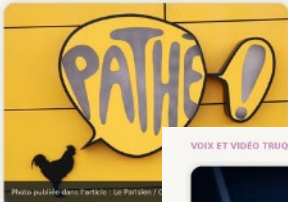
« Ensemble hétéroclite de pratiques d'investigation et d'analyse visant à dévoiler une information préalablement dissimulée en récoltant, croisant ou analysant des données numériques disponibles en source ouverte »

Kevin Limonier et Maxime Audinet

Ou **ROSO** en français, soit «
renseignement d'origine
sources ouvertes ».

Pourquoi ça nous concerne ?

FRAUDE AU PRÉSIDENT



Faux virements : Pathé perd 19,2 M€

En mars 2018, des escrocs se sont fait passer pour la direction du groupe Pathé afin d'obtenir des virements de sa filiale néerlandaise.

Photo publiée dans l'article : Le Parisien / C. L.

Article : Le Parisien, 10 novembre 2018
Synthèse rédigée à partir de l'article cité. Voir

VOIX ET VIDÉO TRUQUÉES



Deepfake : l'arnaque passe à la vitesse supérieure

Faux visages, vidéos et messages audio peuvent rendre crédible une demande de virement.

Photo publiée dans l'article : Getty Images

Article : Le Parisien, 29 mai 2024
Synthèse rédigée à partir de l'article cité. Voir

DÉSINFORMATION ET RÉPUTATION



Faux communiqué : Vinci décroche en Bourse

Le 22 novembre 2016, un faux communiqué annonçant de graves irrégularités comptables.

Photo publiée dans l'article : AFP / S. B.

Article : AFP Making-of, 1er décembre 2016
Synthèse rédigée à partir de l'article cité. Voir

ESPIONNAGE ÉCONOMIQUE



Technologies sensibles : l'affaire Ommic

Dans l'affaire Ommic, la justice enquête sur des soupçons de transfert de procédés et de données sensibles.

Photo publiée dans l'article : IP3 / M. C.

Article : Le Parisien, 26 juillet 2023
Synthèse rédigée à partir de l'article cité. Voir

RISQUES PHYSIQUES ET ENLEVEMENTS



Cryptomonnaies : la menace des enlèvements

Selon la police judiciaire, les enlèvements et séquestrations liés aux cryptomonnaies se sont multipliés. Les cibles sont notamment des professionnels du secteur ou des détenteurs d'actifs numériques. Depuis le début de 2026, plus de quarante faits ont été recensés en France.

Photo publiée dans l'article : LP / Fred Dugit

Article : Le Parisien, 16 avril 2026
Synthèse rédigée à partir de l'article cité. Visuel de présentation, sans reprise de la mise en page de média.

REPERE

> 40 faits

recensés depuis janvier 2026

Fraude : 123 000 \$ de pertes déclarées
par plainte aux USA en 2025

D'après les données de l'IC3 du FBI

À VOUS DE JOUER



WIGLE



SHODAN



PIMEYES



HAVEIEENPWNED



Solution : Réduire son exposition



Utiliser un gestionnaire de mots de passe

(Bitwarden, 1Password, Keepass...)



Maîtriser ses appareils connectés



Se faire anonymiser au guichet unique de l'INPI



Effacer ses comptes et photos de profil qui ne servent plus



Élaborer une phrase de passe, contre les hypertrucages (deepfake)



Contacter le 17Cyber en cas d'attaque avérée

SUIVEZ-NOUS



 [OVIDE](#)

contact@ovide.fr

www.ovide.fr





La Région
Auvergne-Rhône-Alpes



ATOOUTS 
NUMÉRIQUES

**Les bons réflexes pour
protéger un
établissement
touristique**

Financé par



La Région
Auvergne-Rhône-Alpes



Cofinancé par
l'Union européenne

Opéré par

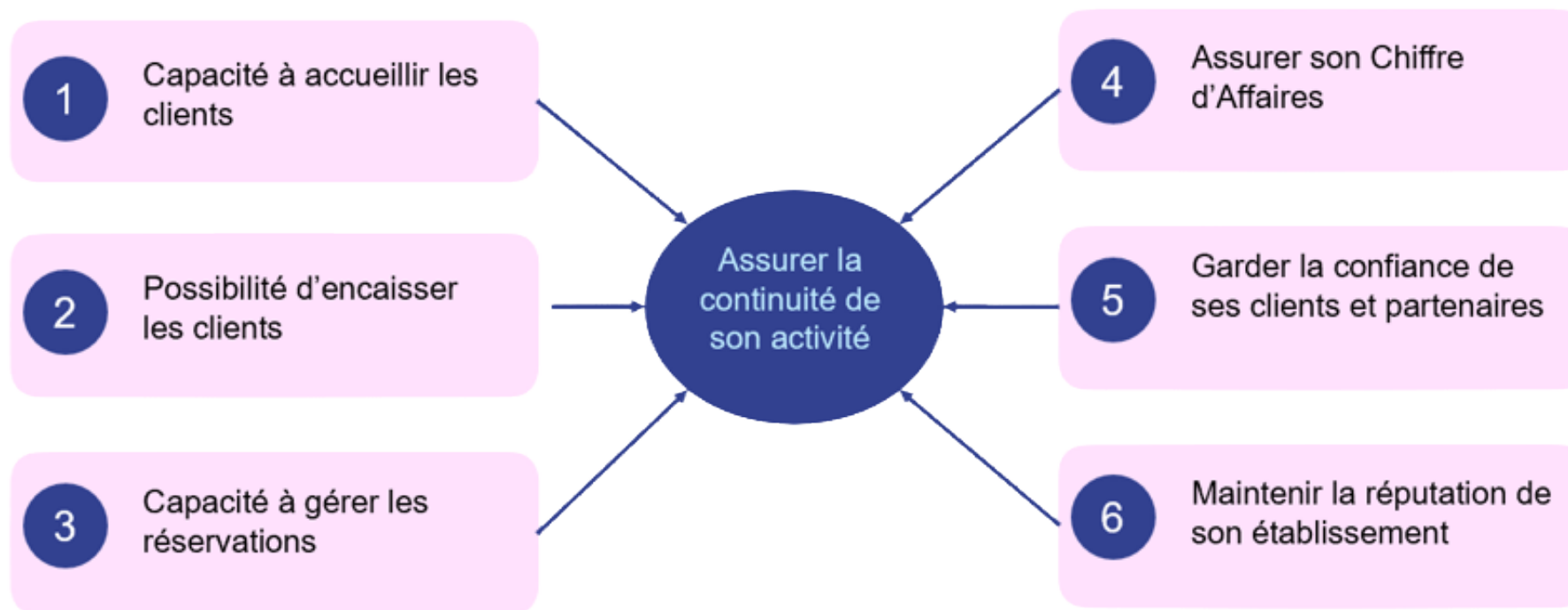
ene
experts du numérique en entreprises
Auvergne-Rhône-Alpes

Dans le cadre des actions du

CAMPUS RÉGION
DU NUMÉRIQUE



La cybersécurité protège votre activité

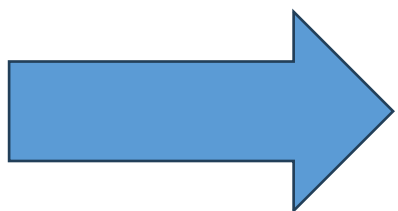


Mon entreprise pourrait-elle continuer à fonctionner si ses outils numériques étaient indisponibles pendant deux ou trois jours ?

Les 4 attaques les plus courantes dans le secteur du tourisme :



1. Faux message d'une plateforme de réservation
2. Le faux changement de coordonnées bancaires
3. Le logiciel de réservation inaccessible
4. Le compte de messagerie piraté



Hygiène informatique : Huit règles prioritaires

1. Protéger les comptes importants

Les comptes numériques représentent souvent la principale porte d'entrée dans l'entreprise. La messagerie doit être protégée en priorité. Une personne qui accède à votre boîte électronique peut lire vos échanges, contacter vos clients, demander la réinitialisation d'autres mots de passe ou préparer une fraude.

Les bonnes pratiques :

- Utilisez un mot de passe différent pour chaque service important,
- Choisissez des mots de passe longs,
- N'utilisez pas le nom de l'entreprise, l'année en cours ou le nom de l'activité,
- Ne conservez pas les mots de passe sur un papier visible,
- Utilisez un gestionnaire / coffre-fort de mots de passe,
- Ne partagez pas les mots de passe,
- Activez la double authentification*,
- Ne communiquez jamais un code reçu par SMS à une autre personne.

2. Effectuer des sauvegardes régulières

Une sauvegarde est une copie des données importantes, conservée pour pouvoir les récupérer après une panne, une erreur, un vol ou une cyberattaque. Sauvegardez en priorité les réservations, les fichiers clients, les factures, les documents comptables, les contrats et les plannings.

- **Une sauvegarde doit être vérifiée** : il ne suffit pas qu'un message indique «sauvegarde terminée». Il faut vérifier régulièrement qu'un fichier peut réellement être récupéré. Par exemple, tous les trois mois, choisissez un document sauvegardé et demandez à votre prestataire de le restaurer.
- **Attention aux supports constamment connectés** : si un disque de sauvegarde reste branché en permanence à l'ordinateur, un logiciel malveillant peut également bloquer les fichiers présents sur ce disque. Il est donc préférable de disposer d'au moins une sauvegarde déconnectée ou protégée contre la modification.

3. Installer les mises à jour

Les mises à jour ne servent pas uniquement à ajouter de nouvelles fonctions. Elles corrigent aussi des défauts de sécurité. Un équipement ou un logiciel ancien peut contenir une faiblesse connue et facilement utilisée par un cybercriminel.

- Les mises à jour concernent entre autres : les ordinateurs, les smartphones, les logiciels utilisés en local, les navigateurs Internet, la box et les équipements réseau, l'outil de mise à jour du site Internet, etc...
- Lorsque cela est possible, activez les mises à jour automatiques.
- Les équipements ou logiciels qui ne reçoivent plus de mises à jour doivent être remplacés ou isolés du reste du réseau.

4. Apprendre à reconnaître un message suspect

Un message doit attirer votre attention lorsqu'il :

- Crée un sentiment d'urgence,
- Menace de fermer un compte,
- Annonce un paiement refusé,
- Signale une réservation inhabituelle,
- Demande un mot de passe,
- Demande de modifier un compte bancaire,
- Contient une pièce jointe inattendue,
- Propose une offre trop avantageuse,
- Présente des fautes ou une mise en page inhabituelle.

En cas de doute :

1. Ne cliquez pas immédiatement,
2. Vérifiez l'adresse complète de l'expéditeur,
3. Contactez directement la personne ou l'organisme,
4. Connectez-vous depuis le site ou l'application habituelle,
5. Demandez l'avis d'un collègue ou du prestataire informatique.

5. Protéger les ordinateurs, smartphones et tablettes

Mesures simples à mettre en place :

- Activez le verrouillage automatique de l'écran,
- Ne laissez jamais une session ouverte dans un espace accessible au public, (⌘+L pour verrouiller)
- Installez une solution de protection adaptée (antivirus ou solution de sécurité),
- Utilisez un filtre de confidentialité sur vos écrans,
- Ne branchez pas une clé USB inconnue,
- N'installez pas un logiciel sans vérifier son origine,
- Évitez d'utiliser l'ordinateur professionnel pour des usages personnels,
- Signalez immédiatement la perte ou le vol d'un appareil.



6. Séparer le Wi-Fi des clients du réseau professionnel

Proposer une connexion Wi-Fi aux visiteurs est devenu courant voire obligatoire dans certaines activités. Mais le réseau utilisé par les clients ne doit pas être le même que celui des équipements professionnels.

Demandez à votre prestataire de vérifier que :

- Les deux réseaux sont bien séparés,
- Les informations techniques des connexions des clients sont tracées pour respecter les obligations légales,
- Le mot de passe d'administration de la box a été changé,
- Les équipements réseau sont à jour,
- Les appareils sensibles ne sont pas accessibles depuis le Wi-Fi client

7. Gérer les accès des salariés, stagiaires et saisonniers

Le tourisme emploie souvent des salariés saisonniers ou temporaires. Il est important d'organiser leurs accès dès leur arrivée et de les supprimer à leur départ.

À l'arrivée :

- Créez un compte individuel,
- Donnez uniquement les accès nécessaires,
- Expliquez les règles essentielles et former les sur les logiciels utilisés,
- Précisez comment signaler un message suspect,
- Évitez de partager le mot de passe du responsable,

Au départ :

- Désactivez le compte,
- Récupérez les équipements et les badges,
- Retirez l'accès à la messagerie et aux logiciels,
- Pensez aux accès à vos réseaux sociaux et services en ligne,
- Changez les codes qui ont été partagés

8. Se préparer en cas d'incident

Même une entreprise bien protégée peut rencontrer un problème. L'objectif est alors de limiter les dégâts et de reprendre l'activité rapidement.

Préparez une fiche simple contenant :

- Le nom de la personne à prévenir,
- Les coordonnées du prestataire informatique,
- Le numéro de la banque,
- Les coordonnées de l'assureur,
- Les accès aux sauvegardes,
- Les coordonnées des principales plateformes,
- Les consignes à suivre,
- Les solutions permettant de fonctionner temporairement sans informatique.



Retrouvez tous les conseils ici



Ainsi que le formulaire 17 CYBER

Financé par



Cofinancé par
l'Union européenne

Opéré par



Dans le cadre des actions du

CAMPUS RÉGION
DU NUMÉRIQUE

Les centres de ressources :

Le Campus Cyber Régional : <https://campusnumerique.auvergnerhonealpes.fr/>

Le programme ATOUTS Numérique :
<https://campusnumerique.auvergnerhonealpes.fr/programme-atouts-numeriques/>

Cyber Assistance Auvergne-Rhône-Alpes : <https://www.cyber-assistance-aura.fr/>

Cybermalveillance : <https://www.cybermalveillance.gouv.fr/>

L'ANSSI : <https://cyber.gouv.fr/>



Merci