

DLP (Data Loss Prevention) Protection contre la fuite des données sensibles



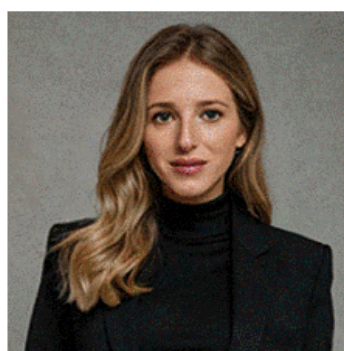
Par webinaire Zoom

Lundi 7 avril
18h00 - 20h00



Protection contre la fuite de données

Le DLP (Data Loss Prevention)



Keren BISMUTH
Softteam Consulting
société de conseil
du groupe Docaposte

Organisateurs



Université
Paris Cité



Béatrice Laurent



Gérard Peliks



Des menaces pèsent sur vos données sensibles

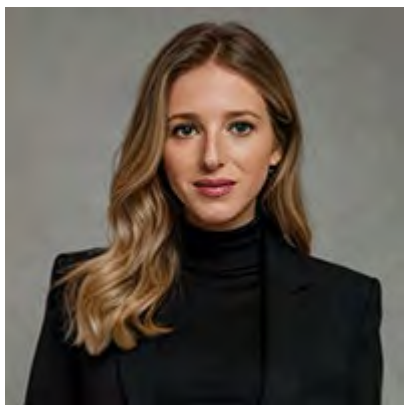
Vous pouvez accéder sur place ou par l'Internet à vos données personnelles, comme vos données d'identité, vos données financières, vos données de santé... **Il faut les protéger** car des individus malveillants peuvent réussir comme vous à y accéder. Des pare-feux, entre autres outils de cybersécurité, sont indispensables mais sont très loin d'être suffisants.

Les données appartenant à votre organisation, les données dont vous êtes dépositaires, peuvent être utilisées, suite à des cyberattaques sensibles réussies, à une exfiltration, suivie de demandes de rançon ou d'atteinte grave à la réputation de votre organisation. **Il faut les protéger.**

Et peut-être que ces données sont-elles déjà en vente sur les marchés noirs de la cybersécurité ou accessibles sur des réseaux sociaux ? Il aurait dû les avoir protégés quand il était encore temps...

Il faut protéger vos données sensibles, mais comment ? C'est l'ambition du DLP. Une experte de ces technologies, et des méthodes à mettre en place, nous présentera le Data Loss Prevention.

Je donne la plume à l'intervenante Keren BISMUTH



La cybersécurité et protection des données professionnelles représente **l'enjeu le plus crucial** pour les entreprises. Elles sont le patrimoine de celle-ci. La donnée peut apporter à diverses informations suivant son interprétation et son contexte. Les résultats qui en découlent sont importants tant pour la survie, la protection mais surtout la valorisation de l'entreprise.

Le DLP (Data Loss Prevention) *Prévention contre la perte de données* représente à la fois une garantie mais également un contrôle des envois de données vers l'extérieur tout en devant allier légitimité, disponibilité et couverture de ceux-ci. Aujourd'hui, avec les nouvelles contraintes technologiques, les intérêts personnels mais surtout l'affûtage constant des données il est plus que nécessaire de se montrer à la hauteur de leur supervision.

Anticiper la fuite d'information repose à la fois sur la technique mais également sur la stratégie. Il est nécessaire de savoir classifier ses données, connaître son métier, évaluer le risque de chaque fuite de données potentielles, les recours par la suite. Les moyens mis en place doivent être transparents pour les collaborateurs et confidentiels pour les administrateurs.

Comment allier confidentialité de la donnée, intégrité et disponibilité des services en mettant en place une solution DLP ? Quels sont les paramètres à prendre en considération ? Quelles sont les questions qui feront pencher la balance sur les prises de décision tout au long du cycle de vie de cette mise en place de ce produit ?

Je reprends la plume

Qui est Keren BISMUTH ?

Keren Bismuth est consultante en cybersécurité en charge de mission DLP (Data Loss Prevention) chez **SOFTEAM** consulting, société de conseil du groupe DOCAPOSTE (Groupe La Poste).

Keren est ingénieure et diplômée du MBA Management de la Cybersécurité de *deVinci Executive Education*, promotion 2021. Sur la photo que j'ai pris avec mon smartphone, voici Keren en habit de cérémonie, lors de la remise des diplômes des MBA. Un évènement festif dans un lieu de rêves, le théâtre des Folies Bergères à Paris.

La photo et puis hop, les chapeaux de l'ensemble des diplômées et des diplômés sont jetés en l'air et retombent, suivant la tradition.



Lisez son post récent en : <https://www.linkedin.com/feed/update/urn:li:activity:7296090818577063936/>

Demande d'inscription au lundi 7 avril, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à Béatrice Laurent :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 7 avril, dès 18 h 00**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants.

Quelques minutes avec le général (2S) Didier Looten, nouveau président de l'ARCSI



Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.



Cette séquence du Lundi de février sera animée par le général (2S) **Didier Looten**.

Didier Looten président de l'ARCSI, nous parlera de cette association et de ses 350 expertes et experts en cybersécurité et en cyberdéfense, et qui va fêter dans 3 ans ses 100 ans d'existence

Il nous présentera en particulier les **16^e Rencontres de l'ARCSI** qui se dérouleront à l'ESIEA (Paris) le jeudi 22 mai sur le thème « **100 ans de Mécanique quantique : quelle Sécurité pour le Cybermonde du XXI^e siècle ?** »

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez, sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php tous les détails, slides, parfois aussi les enregistrements et des comptes rendus, écrits par Clarisse Véron, élève du master2 « Cybersécurité et e-Santé » de l'université Paris Cité.

Par exemple, pour le « Lundi de la Cybersécurité » du mois de février :

La lettre d'invitation est [disponible ici](#).

Les slides de la présentation "Intelligence de la guerre. Renseignement, cyberdéfense, influence" de Bernard BESSON sont [disponibles ici](#).

Les slides du quart d'heure cyber sont [disponibles ici](#).

Le compte-rendu est [disponible ici](#). Ecrit par Clarisse Véron.

La rediffusion (en format YouTube) est [disponible ici](#).

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?
Prompt posé à Gemini (l'IA Générative de Google) :

Comment le DLP protège-t-il nos données ?

La **prévention des pertes de données (DLP)** est une stratégie de sécurité qui vise à empêcher la perte, le vol ou la divulgation non autorisée d'informations sensibles. Voici comment elle protège nos données :

1. Identification et classification des données sensibles

- Les solutions DLP commencent par identifier et classer les données sensibles en fonction de leur contenu, de leur contexte et de leur emplacement.
- Cela peut inclure des informations personnelles identifiables (PII), des données financières, des secrets commerciaux, des informations de propriété intellectuelle, etc.

2. Surveillance et contrôle des données

- Une fois les données sensibles identifiées, les solutions DLP surveillent leur utilisation et leur déplacement à travers différents canaux, tels que les réseaux, les terminaux (ordinateurs portables, smartphones, etc.) et le cloud.
- Elles appliquent des règles et des politiques pour contrôler l'accès, le partage et le transfert de ces données.

3. Prévention des fuites de données

- Les solutions DLP peuvent bloquer ou mettre en quarantaine les actions qui pourraient entraîner une fuite de données, telles que l'envoi d'e-mails contenant des informations sensibles à des destinataires non autorisés, le transfert de fichiers confidentiels vers des périphériques USB ou le partage de données sensibles sur des plateformes de stockage cloud non sécurisées.
- Elles peuvent également chiffrer les données sensibles pour les protéger en cas de perte ou de vol.

4. Détection et alerte

- Les solutions DLP génèrent des alertes en temps réel lorsqu'elles détectent des activités suspectes ou des violations de politique, permettant aux équipes de sécurité de réagir rapidement et de prendre des mesures correctives.
- Elles fournissent également des rapports et des analyses détaillés pour aider les organisations à comprendre les risques de perte de données et à améliorer leurs politiques de sécurité.

5. Conformité réglementaire

- Les solutions DLP aident les organisations à se conformer aux réglementations en matière de protection des données, telles que le RGPD, HIPAA et PCI DSS, en garantissant que les données sensibles sont traitées et protégées conformément aux exigences légales.

En résumé, la DLP protège nos données en :

- Identifiant et classifiant les données sensibles.
- Surveillant et contrôlant l'utilisation et le déplacement des données.
- Prévenant les fuites de données.
- Détectant et alertant en cas d'activités suspectes.
- Facilitant la conformité réglementaire.

Bon, intéressant, mais qu'en pense Keren BISMUTH ? L'interprétation des résultats d'une IA Générative par un expert humain connu et respecté est indispensable pour se faire une opinion. Keren Bismuth nous en dira plus le 7 avril et répondra à nos questions, et nous en discuterons. **Les inscriptions sont ouvertes.**

Gérard Peliks