clearswift
RUAG Cyber Security

Anonymisation contextuelle: suppression des codes actifs et des métadonnées

Principaux composants de la technologie unique et primée d'anonymisation contextuelle de Clearswift.

Qu'est-ce que l'assainissement?

Il s'agit de nettoyer ou purger des fichiers hébergeant du contenu caché dangereux. Ce contenu peut être soit actif (malware) ou de nature informationnelle (propriétés cachées, etc.). Un script invisible et malveillant hébergé sur une page Web pourtant légitime ou embarqué dans un document est un exemple de code dangereux. Pour remédier au problème, il faut supprimer les codes actifs. Du texte sensible caché peut être notamment contenu dans les propriétés d'un document qui contiennent souvent les noms des utilisateurs et des systèmes ainsi que des informations sur les révisions. Qu'il s'agisse de codes ou d'informations cachés, ils doivent être supprimés pour protéger l'entreprise contre des dommages potentiels. L'assainissement est l'une des options proposées par Clearswift pour la prévention contextuelle des fuites de données (A-DLP).

Les options de suppression des codes actifs et des métadonnées sont fournies avec les passerelles Clearswift SECURE et dans la solution ARgon for Email.

De la nécessité de l'assainissement

Suppression des codes actifs (Structural Sanitization): du contenu actif est partout présent. Sa raison d'être est de fournir une expérience plus interactive à l'utilisateur, que ce soit sur Internet ou dans un document. Cependant, les pirates insèrent leur propre contenu actif dans des documents malveillants ou compromis, qu'il s'agisse de documents HTML à télécharger ou de documents PDF en pièces jointes à un email. Tout cela doit être détecté. Dans la mesure où le code actif n'a que rarement une incidence sur le contenu de l'information, il est préférable de tout simplement le supprimer.

Suppression des métadonnées (Document Sanitization): de nombreux documents bureautiques contiennent des données cachées qui pourraient s'avérer sensibles. Il peut s'agir des propriétés d'un document qui peuvent indiquer à la fois le nom de l'auteur et la véritable date du document ou bien de l'historique des modifications qui peut laisser fuir des données sensibles que le ou les auteurs pensaient avoir supprimées, notamment des détails sur le projet, les noms et tarifs des nouveaux produit.

Importance d'un assainissement automatisé

La méthode classique d'assainissement de fichiers consiste en une inspection manuelle ou une suppression des données à l'aide d'un logiciel interne ou d'un logiciel tiers utilisé pour les deux opérations. Néanmoins, dans les deux cas de figure, la réussite de l'opération est conditionnée par l'intervention, souvent négligée, de l'utilisateur ou du département informatique.

Aussi, seul un assainissement totalement automatisé garantit une suppression des codes actifs et des métadonnées à la fois généralisée, homogène et efficace.

L'option d'assainissement des passerelles Clearswift

L'option d'anonymisation proposée par Clearswift est fournie via des expressions et des jetons spécifiés par le client, le tout avec un seuil de détection configurable. Si l'analyse lexicale du contenu atteint le seuil de détection de l'expression, le contenu spécifié est automatiquement anonymisé.

À propos de Clearswift

Clearswift permet à de nombreuses entreprises à travers le monde de protéger leurs informations sensibles afin qu'elles puissent collaborer en toute sécurité et développer leur activité. Notre technologie unique est une solution de prévention des fuites de données simple et "contextuelle" qui limite le risque d'interruption de l'activité tout en permettant aux entreprises d'avoir une visibilité à 100% sur leurs informations critiques à tout moment.

Clearswift est présent dans le monde entier grâce à des sièges régionaux en Europe, Asie-Pacifique et aux États-Unis. Clearswift anime un réseau de partenaires de plus de 900 revendeurs à travers la planète.

Plus d'informations sur
www.clearswift.fr

Royaume-Uni - Siège international
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
United Kingdom
RG7 4SA

Tél: +44 (0) 118 903 8903
Fax: +44 (0) 118 903 9000
Ventes: +44 (0) 118 903 8700
Support technique: +44 (0) 118 903 8200
Email: info@clearswift.com

Australie
Clearswift (Asie/Pacifique) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney
NSW 2060
Australie

Tél: +61 2 9424 1200
Support technique: +61 2 9424 1210
Email: info@clearswift.com.au

Allemagne
Im Mediapark 8
D-50670 Cologne
Germany

Tél: ++49 (0) 221 8282 9888
Support technique: +49 (0) 221 8282 9886
Email: info@clearswift.de

Japon
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo
163-1030
Japon

Tél: +81 (3)5326 3470
Support technique: 0800 100 0006
Email: info.jp@clearswift.com

États-Unis
Clearswift Corporation
309 Fellowship Road,
Suite 200, Mount Laurel,
NJ 08054
États-Unis

Tél: +1 856-359-2360
Support technique: +1 856 359 2170
Email: info@us.clearswift.com

clearswift
RUAG Cyber Security

La fonctionnalité de suppression des métadonnées permet de détecter et de supprimer à la fois les propriétés d'un document et l'historique de révision dans de nombreux types de documents dont les fichiers PDF, Open Office ainsi qu'Office 2007+ Word, Excel et PowerPoint. Il s'agit d'un composant clé de toute solution de prévention contextuelle des fuites de données (DLP) pour protéger contre la fuite de données cachées vers l'extérieur.

La fonctionnalité de suppression des codes actifs s'appuie quant à elle sur la règle de détection du contenu actif (Active Content Detection) et élimine automatiquement le contenu actif tel que les macros VBA des documents Office, les codes de type JavaScript, VBScript et ActiveX du corps des messages HTML et des pièces jointes HTML ainsi que les codes JavaScript et ActiveX des documents PDF.

Anonymisation contextuelle

L'anonymisation contextuelle est une technologie unique et primée de Clearswift qui s'appuie sur une approche proactive de la protection des informations critiques pour empêcher le partage par inadvertance de données sensibles en dehors ou au sein de l'entreprise et atténuer les attaques ciblées entrantes. Pierre angulaire d'une solution de prévention contextuelle des fuites de données, l'anonymisation contextuelle fournit un mécanisme pour contourner l'opération d'arrêt et de blocage des traditionnelles solutions de prévention des fuites de données en supprimant automatiquement et uniquement les informations qui enfreignent les politiques déployées, sans perturber le reste de la communication.

En outre, l'anonymisation contextuelle permet de supprimer du contenu actif potentiellement dangereux d'un document avant que l'utilisateur n'ouvre ce dernier, ce qui garantit un flux de travail sécurisé. Dans de nombreux cas, la réception de documents contenant des menaces persistantes avancées (APT) embarquées peut être facilement enrayée en supprimant le contenu actif dans tous les documents reçus. Les informations légitimes circulent sans entrave tandis que le malware est bloqué.

L'assainissement implique de supprimer tout le contenu dangereux au sein des fichiers. Lorsque ce contenu dangereux comprend du code caché ou obscurci, il peut provoquer la compromission du système par des acteurs externes et entraîner une perte de réputation et de propriété intellectuelle ainsi que d'éventuelles actions de nature réglementaire et des frais de remédiation quant à la faille système. La fonctionnalité d'assainissement de Clearswift empêche tout ceci de manière automatique et centralisée, le tout sans intervention des utilisateurs ni perturbation des processus organisationnels.