Kaspersky Security 9.0 for Microsoft SharePoint Server

Manuel de l'expert en securite de l'information

VERSION DE L'APPLICATION : 9.0

Cher Utilisateur !

Merci d'avoir choisi notre produit. Nous espérons que ce document vous aidera dans votre travail et répondra à la majorité des questions que vous pourriez avoir.

Ce document peut être modifié sans préavis. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.fr/docs.

Date d'édition : 17/10/2014

http://www.kaspersky.com/fr
http://support.kaspersky.com/fr

TABLE DES MATIERES

A PROPOS DE CE DOCUMENT

Le présent document est le manuel d'installation de Kaspersky Security 9.0 for SharePoint Server (ci-après : Kaspersky Security).

Ce manuel est destiné aux experts chargé de la protection des données confidentielle, de la prévention des fuites et des accès non autorisés aux informations, ainsi que de la surveillance continue du système de sécurité de l'information et du support technique des outils employés.

Le manuel vise les objectifs suivants :

- Fournir une aide pour configurer et utiliser Kaspersky Security.
- Offrir un accès rapide aux informations pour répondre aux questions liées au fonctionnement de Kaspersky Security.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir le Support technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document comporte les sections suivantes :

Sources d'informations sur l'application (cf. page 7)

Cette section décrit les sources d'informations sur l'application et indique les sites Internet que vous pouvez utiliser pour discuter de l'utilisation de l'application.

Kaspersky Security 9.0 for SharePoint Server (cf. page 9)

Cette section présente le rôle et les fonctions clés de l'application et décrit également les possibilités d'interaction entre l'utilisateur et l'application.

Exemples d'utilisation de l'application (cf. page 12)

Cette section fournit des exemples d'utilisation des principales fonctions de l'application.

Instructions complémentaires (cf. page 21)

Cette section contient les instructions qui permettent de configurer les paramètres de l'application.

Kaspersky Lab ZAO (cf. page 49)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (cf. page 50)

Cette section reprend des informations relatives au code tiers utilisé dans l'application.

Notice sur les marques commerciales (cf. page 51)

Cette section reprend les informations relatives aux marques citées dans le document et à leurs détenteurs.

CONVENTIONS

Le texte du document contient des éléments sémantiques auxquels nous vous conseillons de prêter attention. Il s'agit d'avertissements, de conseils et d'exemples.

Des conventions stylistiques sont utilisées pour mettre ces éléments en évidence. Le tableau ci-dessous reprend ces conventions ainsi que des exemples d'utilisation.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles pouvant entraîner la perte d'informations, les échecs dans le fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance. Par exemple, les conseils utiles, les recommandations, les valeurs importantes ou les cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés dans un cadre sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Les bases sont obsolètes* survient.	Les éléments sémantiques suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application ;.
Appuyez sur la touche **ENTREE**. Appuyez sur la combinaison de touches **ALT+F4**.	Les noms des touches du clavier sont écrits en caractères majuscules gras. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **ACTIVER**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont écrits en caractères gras.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants de texte apparaissent dans un style spécial (Courier) : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<Nom de l'utilisateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable, sans les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section décrit les sources d'informations sur l'application et fournit des renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher des informations sur l'application :

- page sur le site de Kaspersky Lab ;
- page sur le site du Support technique (banque de solutions) ;
- aide électronique ;
- la documentation.

Si vous ne trouvez pas la réponse à votre question, il est recommandé de contacter le Support Technique de Kaspersky Lab.

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

Page sur le site de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page particulière pour chaque application.

La page (http://www.kaspersky.com/fr/security-sharepoint) fournit des informations générales sur l'application, ses possibilités et les particularités de son fonctionnement.

La page http://www.kaspersky.fr contient un lien vers la boutique en ligne. Où vous pourrez acheter l'application ou renouveler la licence.

Page sur le site du Service d'assistance technique (dans la banque de solutions)

Base de connaissances : rubrique du site du service d'assistance technique contenant des recommandations relatives à l'utilisation des applications de Kaspersky Lab. La Banque de solutions est composée des articles d'aide regroupés selon des thèmes.

La page de l'application dans la Banque de solutions (http://support.kaspersky.com/fr/ksh9) permet de trouver les articles qui proposent des informations utiles, recommandations et réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec l'Anti-virus Kaspersky, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle contient des informations sur chaque fenêtre de l'application, à savoir la liste et la description des paramètres, ainsi que des liens vers les tâches dans lesquelles ces paramètres sont utilisés.

L'aide complète contient les informations détaillées sur l'administration de la protection, la configuration des paramètres de l'application et la résolution des tâches principales de l'utilisateur.

Documentation

La distribution de l'application comprend des documents qui vous permettent d'installer et d'activer l'application sur les ordinateurs du réseau de l'entreprise, ainsi que de configurer ses paramètres de fonctionnement et d'obtenir les informations relatives à l'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.fr).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

KASPERSKY SECURITY 9.0 FOR SHAREPOINT SERVER

L'application Kaspersky Security 9.0 for SharePoint Server (ci-après, l'application) a été développée pour protéger les plateformes SharePoint® contre les virus et autres programmes malveillants. Elle recherche également la présence éventuelle de contenu indésirable sur les sites Internet et protège les informations personnelles des utilisateurs et les données confidentielles de l'organisation sur les sites SharePoint contre les fuites.

Kaspersky Security 9.0 for SharePoint Server offre à l'expert en sécurité de l'information les possibilités suivantes :

- identifier les fuites d'informations en temps réel ;
- bloquer les fichiers contenant des données confidentielles au moment de leur transfert sur le serveur SharePoint ;
- attribuer des priorités aux fuites d'informations sur la base des exigences de la sécurité de l'entreprise ;
- configurer les autorisations de transfert de fichiers sur SharePoint pour certains employés des services de l'organisation ;
- contrôler le traitement des fuites d'informations enregistrées à l'aide d'états ;
- enregistrer et archiver les entrées relatives aux fuites d'informations ;
- définir l'emplacement exact sur SharePoint des fichiers qui contiennent des données confidentielles ;
- envoyer automatiquement par courrier électronique des notifications relatives aux fuites d'informations aux adresses de messagerie électronique ;
- créer automatiquement et manuellement des rapports sur le fonctionnement de l'application et envoyer ceux-ci par courrier électronique à des adresses définies.

DANS CETTE SECTION

PRESENTATION DU SYSTEME DE REPARTITION DES ROLES DANS KASPERSKY SECURITY

Kaspersky Security prend en charge un système de répartition des rôles utilisateur pour gérer les différentes fonctions de l'application. L'accès de l'utilisateur aux fonctions de Kaspersky Security est défini selon les tâches que doit réaliser l'utilisateur.

Kaspersky Security prévoit les rôles suivants :

- **Administrateur** ;
- **Expert en sécurité de l'information**.

Le rôle **Administrateur** est prévu pour l'installation et l'administration de Kaspersky Security. L'administrateur peut gérer les clés, configurer l'application et la mettre à jour. Il peut également configurer la protection antivirus des serveurs SharePoint et l'analyse du contenu Internet.

L'administrateur définit les rôles pour la gestion des différentes fonctions de l'application, réalise l'installation et la configuration initiale de Kaspersky Security pour l'expert en sécurité de l'information. Lors de la configuration initiale, l'administrateur réalise les tâches suivantes :

- Il ajoute une clé active à l'application.
- Il connecte le serveur SharePoint à la console de gestion de Kaspersky Security sur l'ordinateur de l'expert en sécurité de l'information.
- Il active le module DLP dans Kaspersky Security. Ce module est prévu pour la fonction de l'expert en sécurité de l'information.

Avant de commencer à utiliser Kaspersky Security, confirmez que l'administrateur a réalisé la configuration initiale.

Le rôle **Expert en sécurité de l'information** est prévu pour garantir le niveau requis de sécurité d'entreprise sur les ressources Internet SharePoint. L'expert en sécurité de l'information peut gérer la protection des données contre les fuites.

L'expert en sécurité de l'information peut exécuter les actions suivantes dans l'application :

- Créer et modifier les critères d'identification des données confidentielles sur les ressources Internet SharePoint.
- Configurer les modes d'identification des fuites de données et définir les actions que l'application devra exécuter en cas de détection de fuites.
- Configurer la diffusion des notifications relatives aux fuites de données aux adresses de messagerie électronique.
- Consulter les informations détaillées sur les fuites de données.
- Archiver et extraire de l'archive les anciens enregistrements relatifs aux fuites de données.
- Configurer les paramètres de recherche de fichiers contenant des données confidentielles sur les ressources Internet de SharePoint.
- Créer des rapports sur les fuites de données au cours de différentes périodes et configurer la diffusion des rapports aux adresses de messagerie électronique.
- Consulter les rapports prêts sur les fuites de données.

PRESENTATION DE LA PROTECTION CONTRE LES FUITES

Kaspersky Security propose le *module DLP* (Data Leak Protection) qui offre une protection contre les fuites de données. Le composant surveille en temps réel l'envoi par les utilisateurs de fichiers sur SharePoint et identifie les fuites de données selon les critères suivants :

- type et données dans le fichier et leur contenu ;
- nom de l'utilisateur qui envoie le fichier ;
- ressource Internet SharePoint vers laquelle le fichier est envoyé.

Vous pouvez configurer ces paramètres à l'aide de catégories (cf. section « Méthode d'utilisation des catégories. Répartition des données par catégorie » à la page 12) et de stratégies (cf. section « Surveillance et prévention des fuites de données » à la page 14) de l'application.

Si l'utilisateur tente d'envoyer un fichier contenant des données confidentielles (par exemple, des informations relatives aux salaires des employés) sur une ressource Internet SharePoint qui pourrait permettre une fuite de données (par exemple, un portail en accès libre), l'application enregistre cet événement comme une fuite de données.

Si la législation en vigueur dans votre pays impose la notification des citoyens sur le contrôle de leur activité, il faudra informer au préalable les utilisateurs sur le fonctionnement du module DLP.

Vous pouvez définir les actions réalisées par Kaspersky Security en cas de détection d'une fuite de données. L'application peut réaliser automatiquement les actions suivantes :

- créer des *incidents* (enregistrements relatifs à la violation des normes de sécurité de l'organisation) ;
- attribuer des priorités aux incidents sur la base des exigences de la sécurité de l'entreprise ;
- bloquer l'envoi de fichiers sur SharePoint ;
- signaler aux utilisateurs et aux responsables les violations des normes de sécurité de l'entreprise.

Les informations reprises dans les incidents permettent de mener une enquête sur les cas de violation des normes de sécurité de l'entreprise.

EXEMPLES D'UTILISATION DE L'APPLICATION

Cette section fournit des exemples d'utilisation des principales fonctions de l'application. Les exemples contiennent des recommandations relatives à la configuration de la protection des données contre les fuites et à l'utilisation des incidents et des rapports ainsi que des liens vers des instructions complémentaires.

DANS CETTE SECTION

METHODE D'UTILISATION DES CATEGORIES. REPARTITION DES DONNEES PAR CATEGORIE

L'application utilise des catégories pour contrôle les fuites de données sur les sites SharePoint et pour rechercher les informations sur ces sites. Les catégories reprennent les critères selon lesquels l'application identifie sur les sites SharePoint les données couvertes par la stratégie de sécurité de l'organisation.

Commencez à utiliser l'application en réalisant une analyse des données à protéger contre les fuites et en les répartissant en catégories.

Cet exemple d'utilisation de l'application vous expliquer comment répartir les données par catégorie et comment utiliser ces catégories pour contrôler les fuites de données et pour rechercher des informations sur les sites SharePoint. Avant de commencer, découvrez les termes principaux utilisés dans cet exemple :

- Une *catégorie* désigne un ensemble de critères d'identification des données sur les sites SharePoint.
- Les *données tabulaires* désignent les informations organisées dans un tableau. La méthode la plus répandue de conservation des données du tableau est un fichier au format CSV (abréviation anglaise de Comma Separated Values, valeurs séparées par des virgules).
- Les *mots clés* sont des mots, des expressions ou des ensembles de caractères qui permettent à l'application d'identifier les données sur les sites SharePoint.
- Les *catégories de Kaspersky Lab* sont des catégories préparées par les experts de Kaspersky Lab.

Exemples d'exécution d'une tâche :

1. Sélectionnez les données couvertes par la stratégie de sécurité de l'organisation et répartissez-les en groupe selon des caractéristiques communes (par exemple, comptabilité, données personnelles ou innovations). Sélectionnez les critères qui distinguent ces données des autres (par exemple, données enregistrées dans des tableaux ou données contenant le nom de nouvelles technologies ou de nouveaux produits).

2. Sur la base des critères sélectionnés et des caractéristiques générales, sélectionnez les types de catégorie à utiliser dans l'identification des données :

   - Pour identifier les données conservées dans des tableaux (par exemple, données personnelles des employés, informations relatives aux salaires et aux cartes bancaires), utilisez les catégories de données tabulaires (cf. section « Ajout d'une catégorie de données tabulaires » à la page 26). L'application identifie les données sur la base du nombre de correspondances avec les cellules du tableau défini dans la catégorie.

   - Pour identifier les informations sous forme de texte (par exemple, les informations sur les technologies ou les processus de la société), utilisez les catégories de mots clés (cf. section « Ajout d'une catégorie de mots clés » à la page 25). L'application identifie les données sur la base des termes clés ou des expressions composées de plusieurs termes clés repris dans la catégorie.

   - Catégories prédéfinies de Kaspersky Lab (à la page 13).

   Vous pouvez utiliser les catégories pour la surveillance et la prévention des fuites de données (cf. section « Surveillance et prévention des fuites de données » à la page 14) et pour la recherche de données sur les sites SharePoint (cf. section « Configuration des paramètres du rapport par stratégie et par incident » à la page 37).

CATEGORIES DE KASPERSKY LAB

Les *catégories de Kaspersky Lab* sont des catégories préparées par les experts de Kaspersky Lab.

Tableau 1. Catégories de Kaspersky Lab

ZONE DE DONNEES	NOMS DES CATEGORIES	DESCRIPTION DES CATEGORIES
Données des cartes de paiement	**Cartes de paiement**	Cette catégorie permet de rechercher dans les fichiers la présence éventuelles de données protégées par la norme internationale de sécurité applicable aux données du secteur des cartes bancaires PCI DSS (Payment Card Industry Data Security Standard). Cette norme doit être adoptée par les sociétés qui utilisent des systèmes de paiement et qui doivent protéger les données personnelles des titulaires des cartes lors du traitement, du transfert et de l'enregistrement des données.
Données personnelles	**Données personnelles (Grande-Bretagne)** **Données personnelles (Allemagne)** **Données personnelles (Russie)** **Données personnelles (Etats-Unis)**	Les catégories permettent de rechercher dans les fichiers la présence de données qui permettraient d'identifier un individu ou de le localiser (par exemple, date de naissance, adresse du domicile, données du passeport ou du permis de conduire, numéro de sécurité sociale, données relatives aux cartes bancaires et aux numéros de compte et autres informations). La nature des données considérées comme confidentielles dépend de la législation du pays dont l'utilisateur est citoyen.

ZONE DE DONNEES	NOMS DES CATEGORIES	DESCRIPTION DES CATEGORIES
Données médicales	**Données médicales (Grande-Bretagne)** **Données médicales (Allemagne)** **Données médicales (Russie)** **Données médicales (Etats-Unis)** **Données médicales (France)**	Ces catégories permettent de rechercher dans les fichiers la présence éventuelles de données relatives aux numéros de police d'assurance, aux antécédents médicaux des patients, aux diagnostics et aux recommandations des médecins. Les ensembles de données sur les médicaments, les procédures médicales et sur la couverture sociale dépendent du pays dans lequel l'individu bénéficie d'une assistance médicale. Les marques commerciales et les marques de service enregistrées appartiennent à leurs propriétaires respectifs.
Données protégées par la législation	**Loi fédérale N152**	Cette catégorie permet de rechercher dans les fichiers la présence de données protégées par la loi n°125 de la Fédération de Russie. La loi garantit la protection des données personnelles pendant le traitement et l'utilisation. Ces exigences doivent être respectées par les *exploitants de données personnelles* et régissent la collecte, le traitement, l'enregistrement et le transfert des données personnelles.
	Loi fédérale HIPAA	Cette catégorie permet de rechercher dans les fichiers la présence de données protégées par la loi HIPAA (The Health Insurance Portability and Accountability Act) des Etats-Unis. Cette loi vise à protéger la confidentialité des données relatives à l'état physique et psychique des malades. Ces dispositions concernent les institutions médicales et les travailleurs médicaux qui transfèrent par voie électronique des informations sur l'état des patients.
Données de documents administratifs	**Documents administratif (Russie)**	Cette catégorie permet de vérifier si les fichiers appartiennent aux documents administratifs et réglementaires utilisés dans l'activité des sociétés russes (par exemple, décrets, descriptions de fonction, documents cadre).
Données de documents confidentiels	**Documents confidentiels (Russie)**	Cette catégorie permet de rechercher dans les fichiers la présence de conventions qui limitent la diffusion du document à un groupe restreint de personnes (par exemple, « usage interne uniquement », « secret », « confidentiel »).
Données de documents financiers	**Documents financiers (Russie)**	Cette catégorie permet de vérifier si les fichiers appartiennent aux documents financiers utilisés dans l'activité des sociétés russes (par exemple, commandes, factures, avis de paiement).

SURVEILLANCE ET PREVENTION DES FUITES DE DONNEES

Vous pouvez surveiller et prévenir les fuites de données sur les sites SharePoint à l'aide de la fonction de contrôle des fuites de données.

Avant de réaliser cette tâche, il est conseillé de consulter les exemples dans « Méthode d'utilisation des catégories de données ».

Une *stratégie* est une forme d'indiquer à l'application les critères d'identification de fuites de données et les actions à réaliser en cas de détection d'une telle fuite. La stratégie contient un ensemble de paramètres de l'application pour le contrôle des fuites de données de la catégorie définie sur les sites SharePoint. L'application utilise les stratégies pour contrôler l'interaction des utilisateurs avec les fichiers sur les sites SharePoint. Si l'utilisateur tente d'accéder à des données qui ne correspondent pas à ses fonctions, l'application signale une *violation de la stratégie*.

Une stratégie est définie pour une catégorie de données. Il est possible de définir plusieurs stratégies pour une catégorie.

Cet exemple d'utilisation de l'application vous apprendra à surveiller et à prévenir les suites de données sur les sites SharePoint. Avant de commencer, découvrez les termes principaux utilisés dans cet exemple :

- Une *stratégie* est une forme d'indiquer à l'application les critères d'identification de fuites de données et les actions à réaliser en cas de détection d'une telle fuite.

- Une *violation de la stratégie* est un événement dans le fonctionnement de l'application qui indique une fuite éventuelle de données. L'utilisateur viole la stratégie s'il charge par exemple sur SharePoint des données qui ne lui étaient pas destinées.

Exemples d'exécution d'une tâche :

Avant d'exécuter cette tâche, il est conseillé de créer les catégories selon lesquelles l'application va surveiller et prévenir les fuites de données (cf. section « Méthode d'utilisation des catégories. Répartition des données par catégorie » à la page 12).

1. Sélectionnez la catégorie qui définit les données que vous souhaitez contrôler.

2. Définissez les critères d'identification d'une fuite de données correspondantes à la catégorie sélectionnée : quels sont les utilisateurs qui ne peuvent pas charger les données, quels sont les utilisateurs qui peuvent charger les données à titre d'exception et quels sont les sites sur lesquels les utilisateurs ne peuvent pas charger les données.

3. Établissez une ou plusieurs stratégies pour cette catégorie (cf. section « Assistant de création d'une stratégie » à la page 32).

   Dans les paramètres de la stratégie, définissez les utilisateurs qui ne peuvent pas charger les fichiers contenant les données qui correspondent à la catégorie sélectionnée.

La stratégie sera active sur les sites SharePoint sélectionnés dès son ajout. L'application surveillera les données dans les fichiers et créera des incidents en cas de violation de la stratégie.

S'il faut prévenir tous les types de fuites de données possibles, cochez la case **Bloquer le fichier** dans les paramètres de la stratégie. Dans ce cas, l'utilisateur ne pourra pas charger le fichier. L'application enverra alors automatiquement une notification sur la violation de la stratégie à l'adresse électronique de l'utilisateur. Cette option est conseillée si la probabilité d'une fuite de données lors du chargement du fichier est élevée.

RECHERCHE DE DONNEES SUR DES SITES SHAREPOINT

La recherche de données permet d'analyser les fichiers situés sur les sites SharePoint et d'y rechercher la présence de données appartenant à des catégories définies.

La recherche de données vous permet d'effectuer les tâches suivantes :

- Identifier tous les sites SharePoint sur lesquels sont actuellement conservées des fichiers contenant des données de catégories.

- Analyser quand vous le souhaitez les sites SharePoint et y rechercher la présence de fichiers contenant des données appartenant à des catégories définies. Par exemple, vous pouvez obtenir des informations sur des fichiers contenant des données financières ou des données personnelles sur des collaborateurs situés à un emplacement inapproprié.

- Rechercher sur SharePoint des fichiers définis à l'aide des catégories de données. Par exemple, vous pouvez rechercher un fichier dont vous ignorez le nom ou le format mais dont vous connaissez le type de données contenues ou l'emplacement sur un site SharePoint.

La charge sur les serveurs SharePoint indiqués dans les paramètres de la tâche augmente lors de la recherche de données. Cela peut entraîner un déséquilibre de la charge sur les serveurs et une rupture des connexions avec le serveur. Afin de maintenir l'équilibre de la charge, l'administrateur peut limiter la liste des serveurs SharePoint sur lesquels pourront être lancées les tâches de recherche. Si après le lancement de la tâche, la colonne **État** affiche le message *Aucun serveur accessible*, adressez-vous à l'administrateur afin d'obtenir les autorisations pour le lancement de la tâche.

Administration des tâches de recherche

Le recherche de données sur les sites SharePoint est effectuée sous la forme de tâches de recherche (cf. section « Ajout d'une tâche de recherche » à la page 24).

Vous pouvez configurer les paramètres suivants pour chacune des tâches :

- catégories de données selon lesquelles la recherche est effectuée ;
- sites SharePoint sur lesquels la recherche est effectuée ;
- mode et planification du lancement de la tâche ;
- actions de l'application en cas de détection de fichiers correspondant aux critères de recherche.

  En cas de détection de fichiers, l'application peut créer des incidents et consigner les informations sur l'événement dans le journal des événements Windows®.

Vous pouvez ajouter plusieurs tâches de recherche afin de pouvoir rechercher la présence de fichiers contenant des données de plusieurs catégories sur plusieurs sites SharePoint. Si nécessaire, vous pouvez modifier les paramètres de la tâche de recherche (cf. section « Modification des paramètres de la tâche de recherche » à la page 28).

Si les catégories de données sélectionnées pour la recherche sont modifiées pendant la recherche (par exemple, suppression de mots-clés ou ajout de nouvelles données tabulaires), l'application poursuivra la recherche des fichiers en appliquant les modifications apportées aux catégories de données. L'application n'analyse qu'une seule fois les fichiers détectés.

L'application exécute la recherche en arrière plan. Quelle que soit la planification du lancement de la tâche de recherche, vous pouvez lancer ou arrêter la tâche à tout moment (cf.section « Lancement et arrêt de la recherche de données » à la page 28).

L'application n'analyse pas les fichiers système lors de la recherche.

La progression de la tâche est matérialisée par un indicateur. L'indicateur affiche le pourcentage de fichiers analysés par rapport au nombre de fichiers stockés sur les sites SharePoint sélectionnés.

Traitement des résultats de la recherche

Une fois la tâche de recherche exécutée, l'application crée un rapport sur les résultats de la recherche (cf. section « Consultation des résultats de la recherche » à la page 44).

Chaque rapport contient un tableau contenant la liste des fichiers correspondant aux paramètres de la recherche. Le nom du rapport est généré automatiquement et correspond au nom de la tâche pour laquelle il a été créé.

Si nécessaire, vous pouvez enregistrer le rapport afin de pouvoir consulter les informations sur les résultats de la recherche sans ouvrir la Console d'administration (cf.section « Enregistrement des résultats de la recherche » à la page 46).

Les résultats de la recherche peuvent être utilisés afin d'analyser l'état actuel de la protection des données sur SharePoint et d'apporter des modifications éventuelles à la stratégie.

TRAITEMENT DES INCIDENTS

Un incident est une entrée relative à un événement survenu pendant le fonctionnement de l'application et lié à une fuite possible d'informations. Kaspersky Security crée des incidents dans les cas suivants :

- violation d'une stratégie ;
- recherche des données sur SharePoint.

Chaque incident contient des informations détaillées sur les fichiers et les utilisateurs impliqués ainsi que sur son origine. Ces informations sont indispensables pour analyser les fuites de données éventuelles et mener une enquête.

Le traitement des incidents dépend des attribution de l'expert en sécurité des informations et peut varier en fonction des procédures de traitement des incidents en vigueur dans l'organisation.

Gestion du traitement des incidents

Le traitement des incidents peut être géré d'une des manières suivantes :

- à l'aide des états des incidents ;

  L'état de l'incident affiche les informations relatives à l'état actuel de l'incident. Vous pouvez modifier l'état d'un incident à tout moment. Les informations relatives à la modification de l'état d'un incident, à l'auteur de la modification et à l'heure de la modification sont consignées dans l'historique de l'incident.

  L'application permet de modifier l'état de plusieurs incidents simultanément (cf.section « Modification de l'état d'un incident » à la page 30).

- à l'aide de commentaires.

  Les commentaires peuvent contenir des informations sur les causes de la modification de l'état d'un incident et sur l'analyse des circonstances liées à l'incident.

Vous pouvez ajouter des commentaires à un incident pendant la modification de l'état d'un incident ou pendant la consultation de l'historique de l'incident.

Sélection des incidents à traiter

L'application ajoute tous les incidents créés à la liste des incidents dans l'entrée **Incidents**. Vous pouvez modifier l'apparence de la liste des incidents en modifiant les informations sur un incident affichées dans le tableau (cf. section « Modification des informations relatives à un incident affichées dans le tableau » à la page 29).

Quand un incident est créé, l'application lui attribue automatiquement l'état *Nouveau*. Les nouveaux incidents à traiter peuvent être visualisés en mettant à jour la liste des incidents (cf. section « Mise à jour de la liste des incidents » à la page 39).

Pour rechercher des incidents selon des critères définis (par exemple, des incidents liés à un utilisateur donné) vous pouvez utiliser le filtre à incidents (cf. section « Recherche des incidents à l'aide d'un filtre » à la page 39).

Consultation des informations relatives à un incident et traitement de celles-ci

Le traitement de nouveaux incidents peut commencer par la consultation des informations relatives à un incident (cf. section « Consultation des détails d'un incident » à la page 40).

Les incidents sélectionnés pour le traitement doivent avoir l'état *En cours de traitement*. Si plusieurs experts en sécurité de l'information travaillent dans l'organisation, cela simplifie la coordination des tâche.

L'examen du contexte de la violation permet de prendre une décision sur l'incident. Le contexte de la violation contient tous les fragments de texte contenant des données appartenant à une catégorie. Les mots clés ou les données du tableau sont mises en évidence en rouge dans chaque extrait. Si le contexte de la violation ne suffit pas pour prendre une décision sur l'incident, vous pouvez ouvrir le fichier impliqué dans l'incident sur SharePoint.

Fin du traitement des incidents

Après l'analyse des informations relatives à l'incident, celui-ci peut recevoir un des états suivants :

- *Fermé (traité)*, si le traitement de l'incident est terminé.
- *Fermé (faux positif)*, si la violation de la stratégie s'avère être un faux-positif (en cas d'erreur dans la configuration de la stratégie par exemple).
- *Fermé (pas un incident)*, si la violation de la stratégie est acceptable dans le cadre d'une exclusion.
- *Fermé (autre)*, dans tous les autres cas.

Une fois les incidents traités, vous pouvez les retirer de la liste des incidents en procédant à leur archivage (cf. section « Archivage des incidents » à la page 22).

Nouveau traitement d'un incident

Si nécessaire, il est possible d'interagir avec les incidents archivés à l'aide de la restauration des incidents (cf. section « Restauration des incidents depuis l'archive » à la page 23).

L'application attribue l'état *archivé* à tous les incidents restaurés.

Une fois le traitement de ces incidents terminé, vous pouvez les supprimer de la liste (cf. section « Suppression des incidents archivés » à la page 47).

PREPARATION DES RAPPORTS SUR LE FONCTIONNEMENT

Les informations sur le fonctionnement de l'application et l'état de la protection des données contre les fuites peuvent être présentées sous la forme de rapports. Les rapports sont créés sur la base des informations conservées dans la base de données. Ils peuvent être créés manuellement ou automatiquement (selon une planification).

Pour créer des rapports manuellement, vous pouvez utiliser les rapports rapides (cf. section « Génération d'un rapport rapide » à la page 46).

Pour créer des rapports automatiquement, vous pouvez utiliser les tâches de création de rapports (cf. section « Ajout d'une tâche de génération de rapport » à la page 25). Les tâches de création de rapports sont lancées selon la planification établie dans les paramètres de la tâche. Si nécessaire, vous pouvez créer un rapport à tout moment, sans attendre le lancement de la tâche selon la planification (cf. section « Lancement de la tâche de création d'un rapport » à la page 28).

Sélection du type de rapport

Vous pouvez sélectionner le type de rapport en fonction des données que vous souhaitez obtenir :

- Si vous souhaitez recevoir toutes les informations sur les résultats du fonctionnement de l'application et l'état de la protection des données contre les fuites pour une période donnée, créez un *rapport détaillé*. Le rapport contient des informations sur les incidents associés aux catégories et stratégies sélectionnées (cf. section « Configuration des paramètres du rapport détaillé » à la page 35).
- Si vous souhaitez obtenir des informations sur les violations de stratégies par des utilisateurs définis, créez un *rapport par utilisateur*. Le rapport contient des informations sur les incidents associés aux utilisateurs sélectionnés (cf. section « Configuration des paramètres du rapport par utilisateur » à la page 36).

  Ce rapport permet d'analyser la fréquence de violation des stratégies par les utilisateurs. Par exemple, si un utilisateur a violé une stratégie à plusieurs reprises, il faut en informer son directeur.

- Si vous souhaitez vérifier le bon fonctionnement de l'application, créez un *rapport ICP (Indicateurs Clés de Performance, KPI - Key Perfomance Indicators, en anglais) du système.* Le rapport contient des informations sur les indicateurs clés des performances de l'application (cf. section « Configuration des paramètres du rapport ICP (KPI) du système » à la page 37).

  Ce rapport vous permettra de suivre les modifications du fonctionnement de l'application. Si, par exemple, l'application a ignoré une grande quantité de fichiers, cela peut signifier qu'il faut modifier les paramètres de la stratégie.

- Si vous souhaitez vérifier la pertinence de la configuration des stratégies, créez un *rapport par stratégie et par incident*. Le rapport contient des informations sur les incidents associés aux catégories de données sélectionnées (cf. section « Configuration des paramètres du rapport par stratégie et par incident » à la page 37).

  Ce rapport vous permettra d'analyser la corrélation entre les violations de stratégies et les causes de fermeture des incidents. Si, par exemple, les incidents associés à une stratégie sont fermés pour cause de faux-positif, cela peut signifier qu'il faut modifier les paramètres de la stratégie.

Lors de la création d'un rapport détaillé ou d'un rapport par utilisateur, l'application prend en compte les incidents restaurés depuis l'archive.

Traitement des rapports

L'application ajoute tous les rapports créés à la liste des rapports dans le groupe **Consultation et enregistrement des rapports** de l'entrée **Rapports**. Les informations suivantes sont affichées pour chaque rapport :

- nom ;
- date et heure de création ;
- période du rapport ;
- type de rapport.

Ces informations vous aideront à trouver les rapports que vous souhaitez consulter. En cas de création d'un rapport rapide, l'application ouvre automatiquement le rapport créé dans la fenêtre du navigateur défini par défaut.

Si nécessaire, vous pouvez enregistrer les rapports créés afin de les utiliser sans ouvrir la Console d'administration (cf. section « Enregistrement des rapports » à la page 46).

ÉVALUATION DE L'ETAT DE LA PROTECTION DES DONNEES

Pour confirmer que le niveau de sécurité des données sur les sites SharePoint est adéquat, il faut évaluer en permanence l'état de la protection des données. Les informations sur la protection des données sont actualisées en temps réel et s'affichent à l'entrée **Protection des données contre les fuites** (cf. section « **Consultation des informations sur l'état de la protection** » à la page 45).

L'état de la protection des données peut être évalués à l'aide des critères suivants :

- état du module DLP, présence d'erreurs dans le fonctionnement du module ;

  Si le module DLP fonctionne avec des erreurs, cela entraînera une réduction de la protection Si le module DLP est désactivé, l'application n'analyse pas les fichiers lors du transfert sur SharePoint par les utilisateurs.

- statistiques des incidents ouverts ;

  Permet d'évaluer le volume de travail sur les incidents à l'heure actuelle et de planifier le traitement des incidents.

- statistiques des incidents fermés ;

  Permet d'analyser les raisons pour lesquelles des incidents ont été fermés. Les résultats de l'analyse peuvent mettre en évidence les points faibles dans la protection des données et de modifier en conséquence les paramètres des stratégies.

- Statistiques des fichiers transférés vers SharePoint.

  Permet de surveiller et d'évaluer l'efficacité du fonctionnement de l'application.

Vous pouvez configurer l'envoi automatique des notifications sur la modification de l'état de la protection aux adresses de courrier électronique (cf. section « Configuration des adresses de messagerie électronique pour la diffusion des notifications de l'application » à la page 34).

INSTRUCTIONS COMPLEMENTAIRES

Cette section contient les instructions qui permettent de configurer les paramètres de l'application.

DANS CETTE SECTION

ARCHIVAGE DES INCIDENTS

L'*archivage des incidents* est une processus qui permet d'ajouter les incidents dont le traitement est terminé à une archive protégée.

L'archivage des incidents permet de réduire le volume de la base de données SQL® et de réduire la longueur de la liste des incidents affichés dans la console de gestion.

Pour lancer l'Assistant d'archivage des incidents, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Sélectionnez les incidents clos que vous souhaitez archiver.
4. Dans le panneau de résultats de l'entrée, cliquez sur le bouton **Archiver**.

L'application lance l'Assistant d'archivage des incidents.

L'Assistant d'archivage des incidents est composé d'une succession de fenêtres (étapes). Pour naviguer entre les fenêtres de l'Assistant, cliquez sur les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Début de l'Assistant. Sélection des incidents à archiver

La première fenêtre de l'Assistant reprend les informations relatives aux incidents qui vont être ajoutés à l'archive. Seuls les incidents dont l'état est *Fermé* peuvent être ajoutés à l'archive.

Le champ **Chemin d'accès au fichier** doit contenir le chemin d'accès à l'archive à laquelle l'application va ajouter les incidents. Si vous ne désignez pas le nom de l'archive, l'Assistant d'archivage créera une archive avec les incidents. Le nom de l'archive est généré automatiquement et contient la date de création de l'incident le plus ancien et la date de création de l'incident le plus récent. L'application utilise les dates de création des incidents sur le serveur pour composer le nom.

Vous ne pouvez pas archiver des incidents dont l'état est *Nouveau* et *En cours de traitement*, ni des incidents qui ont été restaurés depuis l'archive.

Création d'une archive avec des incidents

Au cours de cette étape, l'Assistant procède à l'archivage des incidents. Une barre de progression apparaît pendant l'archivage des incidents. A l'issue de l'archivage des incidents, l'Assistant passe automatiquement à l'étape suivante.

Fin de l'Assistant.

Lors de cette étape, l'Assistant vous signale la fin de l'archivage des incidents. Il affiche également les informations relatives au nombre d'incidents ajoutés à l'archive. Si des erreurs sont survenues pendant l'archivage, l'Assistant affiche les informations relatives aux incidents qui n'ont pas été ajoutés à l'archive.

Les informations suivantes sont consignées dans l'historique de l'incident :

- nom de l'archive ;
- date et heure d'édition de l'archivage ;
- nom de l'utilisateur qui a réalisé l'archivage.

Les incidents ajoutés à l'archive sont supprimés de la base de données SQL et de la liste des incidents dans l'entrée **Incidents**.

RESTAURATION DES INCIDENTS DEPUIS L'ARCHIVE

La *restauration des incidents* désigne le processus de copie des incidents depuis l'archive vers la base de données SQL.

Vous pouvez restaurer des incidents quand il est nécessaire de consulter les informations relatives à des incidents dont le traitement remonte à il y a longtemps.

Pour lancer l'Assistant de restauration d'incidents, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Dans le panneau de résultats de l'entrée, cliquez sur le bouton **Restaurer**.

L'application lance l'Assistant de restauration des incidents.

L'Assistant de restauration des incidents est composé d'une succession de fenêtres (étapes). Pour naviguer entre les fenêtres de l'Assistant, cliquez sur les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Début de l'Assistant. Sélection des incidents à restaurer

Sélectionnez dans la première fenêtre de l'Assistant les incidents à restaurer.

Indiquez dans le champ **Pour la période** la période au cours de laquelle sont survenus les incidents qui vous intéressent. Le champ **Chemin d'accès au fichier** doit contenir le chemin d'accès à l'archive des incidents à partir de laquelle l'application va restaurer les incidents.

Restauration des incidents

Au cours de cette étape, l'Assistant procède à la restauration des incidents. L'état d'avancement de la restauration des incidents de l'archive apparaît dans la fenêtre de l'Assistant. A l'issue de la restauration des incidents, l'Assistant passe automatiquement à l'étape suivante.

Fin de l'Assistant.

Lors de cette étape, l'Assistant vous signale la fin de la restauration des incidents. Il affiche également les informations relatives au nombre d'incidents restaurés. Si des erreurs sont survenues pendant la restauration, l'Assistant affiche les informations relatives aux incidents qui n'ont pas pu être restaurés.

Un incident qui a été restauré ne peut plus être archivé, ni restauré. Il est impossible de modifier l'état des incidents restaurés.

L'application ajoute tous les incidents restaurés à la liste des incidents dans l'entrée **Incidents**. L'état *archivé* sera attribué aux incidents restaurés.

SELECTION DES CATEGORIES POUR LA GENERATION DES STATISTIQUES PAR INCIDENT

Pour sélectionner les catégories en vue de la création d'un diagramme des statistiques, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Protection des données contre les fuites**.
3. Réalisez une des actions suivantes :
   - Pour créer un diagramme sur les incidents ouverts, cliquez sur le bouton **Sélectionner les catégories** dans le groupe **Incidents ouverts**.
   - Pour créer un diagramme sur les incidents clos, cliquez sur le bouton **Sélectionner les catégories** dans le groupe **Statistiques**.

     La fenêtre **Liste des catégories** s'ouvre.
4. Dans la fenêtre **Liste des catégories**, sélectionnez les catégories de données à inclure dans les statistiques.

   L'application génère les statistiques des incidents selon les catégories que vous avez sélectionnées.

   Si vous cochez la case **Toutes les catégories**, les informations relatives aux nouvelles catégories que vous ajouterez seront ajoutées automatiquement au diagramme des statistiques.
5. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre.

Les données relatives aux incidents générés selon les catégories sélectionnées seront affichées dans le diagramme.

AJOUT D'UNE TACHE DE RECHERCHE

Pour ajouter une tâche de recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Cliquez sur le bouton **Créer** dans le groupe **Tâches de recherche**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Sous l'onglet **Général**, saisissez le nom de la tâche dans le champ **Nom de la tâche**.

5. Dans la liste **Catégories de données à rechercher**, cochez la case des catégories de données dont il faut rechercher des correspondances sur les sites SharePoint.

6. Le cas échéant, cochez les cases **Créer des incidents** et **Consigner les événements dans le journal des événements Windows**.

   En cas de détection de fichiers contenant des données appartenant aux catégories indiquées, l'application crée un incident pour chaque fichier et consigne également les données relatives à la détection des fichiers dans le journal des événements Windows.

7. Sous l'onglet **Mode de lancement**, sélectionnez le mode de lancement de la tâche et configurez sa planification.

8. Sous l'onglet **Sites**, cochez la case en regard des sites SharePoint sur lesquels l'application recherchera les fichiers.

9. Cliquez sur le bouton **OK** pour terminer la création d'une tâche.

La tâche ajoutée apparaît dans le tableau des tâches du groupe **Tâches de recherche**. Vous pouvez exécuter une tâche manuellement après sa création. Si vous avez planifié l'exécution de la tâche, l'application l'exécutera au jour et à l'heure indiqués.

AJOUT D'UNE TACHE DE GENERATION DE RAPPORT

Pour ajouter une tâche de génération de rapport, procédez comme suit :

1. Ouvrez la Console de gestion.

2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.

3. Dans le groupe **Tâches de création de rapports**, cliquez sur le bouton **Nouvelle tâche**.

4. Sélectionnez le type de rapport à créer dans la liste déroulante.

   La fenêtre **Paramètres de la tâche** s'ouvre.

5. Cette fenêtre permet de modifier les paramètres de la tâche de création du rapport.

6. Cliquez sur **OK** pour ajouter la tâche.

La nouvelle tâche apparaît dans la liste des tâches du groupe **Tâches de création de rapports**. L'application lancera la tâche de création des rapports automatiquement selon la planification définie dans les paramètres de la tâche.

AJOUT D'UNE CATEGORIE DE MOTS-CLES

Un *mot-clé* est un mot, une expression ou un ensembles de caractères qui permettent à l'application d'identifier les données sur les sites SharePoint. Pour pouvoir rechercher les données sur les sites SharePoint à l'aide de mots clés, il faut les ajouter à la catégorie. La catégorie peut contenir un mot clé ou une expression contenant plusieurs mots clés.

Pour ajouter une catégorie de mots clés, procédez comme suit :

1. Ouvrez la Console de gestion.

2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.

3. Dans le panneau des résultats de l'entrée, cliquez sur le bouton **Nouvelle catégorie** et dans la liste déroulante des types de catégorie, choisissez l'option **Mots clés**.

   La fenêtre **Paramètres de la catégorie** s'ouvre. La fenêtre permet d'ajouter des mots clés à la catégorie et d'indiquer le nom de la catégorie.

4. Dans le champ de saisie, indiquez les mots clés qui seront repris dans la catégorie.

   Un mot clé est un mot ou une expression repris entre guillemets. Pour tenir compte de la différence entre majuscules et minuscules dans les mots clés, ajoutez le caractère « ! » au début du mot. Les mots-clés peuvent être regroupés en expressions à l'aide des opérateurs : AND, OR, NEAR(n) et ONEAR(n). Pour définir la séquence d'activation des opérateurs, utilisez des parenthèses.

   L'opérateur OR est appliqué automatiquement aux mots clés saisis sur une nouvelle ligne dans le champ. L'application détecte les fichiers dont le texte contient les mots clés d'au moins une ligne de la catégorie.

Exemple :

La catégorie contient l'expression suivante composée de mots clés :

« sécurité » AND (« !Kaspersky Lab » NEAR(5) « code logiciel »)

L'application va détecter les fichiers dont le contenu répond aux critères suivants :

- Les mots et expressions « sécurité », « Kaspersky Lab » et « code logiciel » figurent dans le contenu.
- Les mots « Kaspersky Lab » doivent commencer par une majuscule.
- L'expression « code logiciel » est utilisée avant et après « Kaspersky Lab » dans un intervalle de cinq mots maximum.

Par exemple : « ...protéger le code logiciel de l'application contre le piratage. Kaspersky Lab a présenté lors de la conférence une nouvelle version du produit qui améliorera la sécurité du travail sur réseau ».

   Les détails relatifs à l'ajout d'une catégorie de mots clés sont accessibles via le lien **Aide sur l'ajout de mots clés** dans la fenêtre **Paramètres de la catégorie.**

5. Saisissez le nom de la catégorie dans le champ **Nom de la catégorie**.

6. Saisissez des informations complémentaires en rapport avec les données de la catégorie dans le champ **Commentaires**.

7. Cliquez sur **OK**.

   La nouvelle catégorie sera ajoutée à la liste des catégories dans l'entrée **Catégories et stratégies**.

Vous pouvez utiliser une catégorie pour rechercher des données sur les sites SharePoint et surveiller les fuites de données.

AJOUT D'UNE CATEGORIE DE DONNEES TABULAIRES

Les *données tabulaires* désignent les informations de l'entreprise organisées dans un tableau. La méthode la plus répandue de conservation des données du tableau est un fichier au format CSV (abréviation anglaise de Comma Separated Values, valeurs séparées par des virgules). Les lignes des fichiers CSV correspondent aux lignes du tableau. Les colonnes de tableau dans les fichiers CSV sont séparées à l'aide d'un caractère spécial, le *séparateur de colonnes*. Dans les fichiers CSV, le séparateur de colonne peut être le point virgule.

La recherche des données tabulaires sur les sites SharePoint s'opère à l'aide de la catégorie des données tabulaires. La catégorie contient le chemin d'accès au fichier CSV contenant les données tabulaires à contrôler ainsi que les critères de recherche de ces données.

Le fichier CSV peut être ouvert à l'aide d'applications telles que Notepad, WordPad ou Microsoft Excel®.

Pour ajouter une catégorie de données tabulaires, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Dans le panneau des résultats de l'entrée, cliquez sur le bouton **Nouvelle catégorie** et dans la liste déroulante des types de catégorie, choisissez l'option **Données tabulaires**.

   La fenêtre **Paramètres de la catégorie** s'ouvre. La fenêtre permet d'ajouter des données tabulaires, de configurer les paramètres de recherche et d'indiquer le nom de la catégorie.
4. Dans le champ **Chemin du fichier**, saisissez le chemin d'accès complet au fichier CSV contenant les données tabulaires à ajouter à la catégorie.

   Pour garantir le bon fonctionnement de la catégorie de données tabulaires, le fichier CSV chargé doit être enregistré au format UTF-8.
5. La liste déroulante **Séparateur des colonnes** vous permet de sélectionner le caractère qui sera utilisé comme séparateur des colonnes dans le fichier au format CSV à télécharger :

   La virgule est le séparateur de colonnes par défaut.
6. Définissez le niveau de correspondance avec les données tabulaires.

   Le *niveau de correspondance* désigne le nombre minimum de cellules contenant des données tabulaires dont le contenu doit correspondre aux données dans des fichiers SharePoint. Le nombre de cellules est défini par les croisements uniques des colonnes et des lignes du tableau.

   - Dans la liste **Valeur seuil des lignes**, indiquez le nombre de lignes du tableau.

     Par défaut, l'application trouve les fichiers avec des données présentes dans n'importe quelle paire de lignes du tableau.
   - Dans la liste **Valeur seuil des colonnes**, indiquez le nombre de colonnes du tableau.

     Par défaut, l'application trouve les fichiers avec des données présentes dans n'importe quelle paire de colonnes du tableau.

   Les détails relatifs à l'ajout d'une catégorie de données tabulaires sont accessibles via le lien **Aide sur les paramètres de la recherche** dans la fenêtre **Paramètres de la catégorie.**
7. Saisissez le nom de la catégorie dans le champ **Nom de la catégorie**.
8. Saisissez des informations complémentaires en rapport avec les données de la catégorie dans le champ **Commentaires**.
9. Cliquez sur **OK**.

   Une fenêtre indiqué l'état d'avancement du chargement des données tabulaires dans la catégorie s'ouvre.

   Lors de l'ajout de données tabulaires dans une catégorie, la première ligne du fichier CSV est ignorée (on suppose que la première ligne contient uniquement les titres des colonnes).

   En cas d'erreur lors de l'ajout de données tabulaires à une catégorie, l'application affiche un message reprenant le numéro de la ligne du tableau à l'origine de l'erreur.

   La nouvelle catégorie sera ajoutée à la liste des catégories dans l'entrée **Catégories et stratégies**.

Vous pouvez utiliser une catégorie pour rechercher des données sur les sites SharePoint et surveiller les fuites de données.

LANCEMENT DE LA TACHE DE CREATION D'UN RAPPORT

Pour lancer la tâche de composition du rapport, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Le groupe **Tâches de création de rapports** permet de sélectionner la tâche à lancer.
4. Cliquez sur le bouton **Lancer la tâche**.

L'application crée le rapport conformément aux paramètres configurés dans la tâche. Le rapport apparaît dans la liste des rapports du groupe **Consultation et création des rapports**.

LANCEMENT ET ARRET DE LA RECHERCHE DE DONNEES

Pour lancer ou arrêter une tâche de recherche manuellement, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans la liste des tâches, sélectionnez la tâche de recherche que vous souhaitez lancer ou arrêter.
4. Réalisez une des actions suivantes :

   - Si vous souhaitez lancer une tâche de recherche, cliquez sur le bouton **Démarrer**.

     L'application lance la recherche des données sur les sites SharePoint.

   - Si vous souhaitez arrêter la tâche de recherche, cliquez sur le bouton **Arrêter**.

     L'application arrête l'exécution de la tâche. Lors de l'arrêt de la tâche, l'application crée un rapport qui contient les informations relatives aux fichiers trouvés avant l'arrêt de la tâche. Le rapport s'affiche dans le groupe **Résultats de la recherche**.

Si l'état *Aucun serveur accessible* apparaît dans la colonne **Etat**, cela signifie que les autorisations de lancement de la tâche sur les serveurs repris dans les paramètres de la tâche n'existent pas. Contactez l'administrateur pour résoudre le problème.

MODIFICATION DES PARAMETRES DE LA TACHE DE RECHERCHE

Pour modifier les paramètres d'une tâche de recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans le groupe **Tâches de recherche** de la liste des tâches, sélectionnez la tâche dont vous souhaitez modifier, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Paramètres de la tâche** s'ouvre.

4. Modifiez la tâche dans la fenêtre qui s'ouvre.
5. Cliquez sur **OK** pour enregistrer les modifications.

MODIFICATION DES PARAMETRES DE LA TACHE DE RAPPORT

Pour modifier les paramètres de la tâche de composition d'un rapport, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans le groupe **Tâches de création de rapports**, sélectionnez la tâche, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Modifiez les paramètres de la tâche.
5. Cliquez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UNE CATEGORIE

Pour modifier une catégorie, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Dans la liste des catégories, sélectionnez la catégorie dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Paramètres**.

   La fenêtre des paramètres de la catégorie s'ouvre.
4. Modifiez la catégorie dans la fenêtre qui s'ouvre.

   Les paramètres des catégories de Kaspersky Lab ne peuvent pas être modifiés.
5. Cliquez sur **OK** pour enregistrer les modifications.

MODIFICATION DES INFORMATIONS RELATIVES A UN INCIDENT AFFICHEES DANS LE TABLEAU

Pour modifier les informations relatives à un incident affichées dans le tableau, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.

3. Dans le groupe **Liste des incidents**, cliquez sur le bouton **Sélectionner les colonnes**.

   Le groupe **Sélection des colonnes à afficher** se développe.

4. Dans le groupe, cochez les cases en regard des informations relatives aux incidents qui doivent apparaître dans le tableau.

Les modifications dans le tableau sont appliquées directement après qu'une case a été cochée ou décochée. Les informations relatives à l'incident dont la case a été cochée apparaissent toujours dans le tableau.

MODIFICATION DE L'ETAT D'UN INCIDENT

L'*état de l'incident* affiche les informations relatives à l'état actuel de l'incident. Vous pouvez modifier les états des incidents en fonction du résultat de leur traitement. Les états des incidents interviennent dans la création des rapports de l'application. Il est possible de modifier l'état d'un incident aussi bien dans la liste des incidents que dans la fenêtre des détails de l'incident.

Pour modifier l'état d'un incident, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Dans la liste, sélectionnez l'incident dont il faut modifier l'état.

   Vous pouvez sélectionner un ou plusieurs incidents dans la liste.

4. Cliquez sur le bouton **Modifier l'état**, puis choisissez l'option **Personnalisé** dans la liste déroulante.

   Vous pouvez modifier l'état de tous les incidents dans la liste. Pour ce faire, choisissez l'option **Tous les incidents** dans la liste **Modifier l'état**.

5. Sélectionnez l'état que vous souhaitez attribuer à l'incident ans la liste déroulante **État** de la fenêtre **Modification de l'état** qui s'ouvre.
6. Utilisez le champ **Commentaires** si vous devez indiquer la raison de la modification de l'état ou toute autre information relatives au traitement de l'incident.
7. Cliquez sur **OK** pour enregistrer les modifications.

Le nouvel état de l'incident apparaît dans la colonne **État** de la liste de incidents de l'entrée **Incidents**. Les informations relatives à la modification de l'état et à l'auteur de la modification sont consignées dans l'historique de l'incident.

UTILISATION DES OPERATEURS DE COMPARAISON

Un *mot-clé* est un mot, une expression ou une séquence de caractères indispensable pour permettre à l'application d'identifier des données confidentielles dans un texte.

Les mots et expressions indiqués en tant que mots-clés et placés entre guillemets peuvent être séparés à l'aide d'un espace ou d'un autre caractère (par exemple, « # », « % », « + », « @ », « & », ou par un signe de ponctuation). Les mots-clés peuvent être regroupés en expressions à l'aide des opérateurs : AND, OR, NEAR(n) et ONEAR(n) (cf. tableau ci-dessous).

Tableau 2. Utilisation des opérateurs pour créer des expressions

OPERATEUR	DESCRIPTION DE L'UTILISATION	RESULTAT
!	Le caractère « ! » est utilisé devant un nom pour indiquer qu'il faut tenir compte de la différence entre majuscules et minuscules dans les mots clés. Si le mot clé est une expression qui contient plusieurs mots, l'opérateur de casse est appliqué à chaque mot qui constitue l'expression. **Exemple :** « !Kaspersky Lab »	L'application détectera les fichiers dont le texte contient le mot clé « Kaspersky Lab », commençant par des majuscules. Les fichiers qui contiennent cette expression en minuscules (par exemple, « kaspersky lab ») seront ignorés.
AND	L'opérateur AND permet de trouver deux mots clés ou plus contenus dans le même texte. L'ordre de saisie n'a aucune influence sur la recherche. **Exemple :** « antivirus » AND « sécurité »	L'application identifie les fichiers dont le texte contient à la fois les mots « antivirus » et « sécurité ». Les fichiers contenant un seul de ces mots seront ignorés.
OR	L'opérateur OR permet de trouver dans le texte un des mots clés ou plusieurs mots clés simultanément. **Exemple :** « sécurité » OR « protection de l'ordinateur » L'opérateur OR est appliqué par défaut aux mots clés saisis sur une nouvelle ligne dans le champ.	L'application identifie les fichiers dont le texte contient le mot « sécurité » ou l'expression « protection de l'ordinateur », ou les deux.
NEAR(n)	L'opérateur NEAR permet de trouver plusieurs mots clés espacés de quelques mots dans le texte. Indiquez le nombre de mots qui séparent les mots clés entre parenthèses. **Exemple :** « sécurité » NEAR(6) « système » L'ordre d'utilisation des mots clés n'est pas pris en compte durant la recherche.	L'application identifie les fichiers où le mot « sécurité » est utilisé avant ou après le mot « système », à un maximum de six mots d'écart.
ONEAR(n)	L'opérateur ONEAR permet de trouver plusieurs mots clés espacés de quelques mots dans le texte dans l'ordre indiqué. Indiquez le nombre de mots qui séparent les mots clés entre parenthèses. **Exemple :** « protection » ONEAR(4) « confidentialité »	L'application identifie les fichiers où le mot « confidentialité » est toujours utilisé après le mot « protection », à quatre mots d'écart.

Vous pouvez utiliser plusieurs opérateurs pour définir des expressions complexes de mots clés. Pour définir la séquence d'activation des opérateurs, utilisez des parenthèses.

Exemple :

La catégorie contient l'expression suivante composée de mots clés :

« sécurité » AND (« !Kaspersky Lab » NEAR(5) « code logiciel »)

L'application va détecter les fichiers dont le contenu répond aux critères suivants :

- Les mots et expressions « sécurité », « Kaspersky Lab » et « code logiciel » figurent dans le contenu.
- Les mots « Kaspersky Lab » doivent commencer par une majuscule.
- L'expression « code logiciel » est utilisée avant et après « Kaspersky Lab » dans un intervalle de cinq mots maximum.

Par exemple : « ...protéger le code logiciel de l'application contre le piratage. Kaspersky Lab a présenté lors de la conférence une nouvelle version du produit qui améliorera la sécurité du travail sur réseau ».

La recherche de fichiers à l'aide d'expressions du type « terme1 » NEAR(n) (« terme2 » AND « terme3 ») et « terme1 » NEAR(n) (« terme2 » NEAR(m) « terme3 ») n'est pas prise en charge. La recherche de fichiers selon ce type d'expression entraîne une incertitude dans l'ordre de traitement des parenthèses.

ASSISTANT DE CREATION DE STRATEGIE

Une *stratégie* est une forme d'indiquer à l'application les critères d'identification de fuites de données et les actions à réaliser en cas de détection d'une telle fuite. La stratégie contient un ensemble de paramètres de l'application permettant à cette dernière de contrôler les données de la catégorie sur les sites SharePoint. La configuration initiale des paramètres de la stratégie est effectuée à l'aide de l'assistant de création d'une stratégie.

Pour lancer l'assistant de création d'une stratégie, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Sélectionnez la catégorie de données pour laquelle la stratégie doit être établie.
4. Cliquez sur le bouton **Nouvelle stratégie**.

L'application lance l'assistant de création d'une stratégie.

L'assistant de création d'une stratégie est composé d'une succession de fenêtres (étapes). Pour naviguer entre les fenêtres de l'Assistant, cliquez sur les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

ÉTAPES DE L'ASSISTANT

ÉTAPE 1. FONDEMENT ET ETAT D'UNE STRATEGIE

Cette étape permet de modifier l'état d'une stratégie et d'indiquer le fondement de sa création.

Pour modifier l'état d'une stratégie,

Cochez la case **Activer la stratégie**.

Une fois que l'Assistant aura terminé, l'application contrôlera le transfert de fichiers sur les sites SharePoint conformément aux paramètres définis dans la stratégie.

Pour désigner les fondements de la stratégie,

Le champ **Lien vers le document de référence** accueille le point du document de référence qui garantit la protection des données confidentielles dans l'organisation.

Ces informations sont indispensables pour coordonner le travail de plusieurs experts en sécurité de l'information au sein d'une même organisation.

Saisissez le nom de la stratégie créée dans le champ **Nom de la stratégie**. Si les bords du champ apparaissent en rouge, cela signifie que ce nom a déjà été utilisé pour une autre stratégie.

ÉTAPE 2. CONFIGURATION DES AUTORISATIONS DE TRANSFERT DE FICHIERS

Cette étape vous permet de configurer les autorisations de transfert de fichiers par les utilisateurs vers les sites SharePoint.

Pour configurer les autorisations de transfert de fichiers par les utilisateurs, procédez comme suit :

1. Dans la liste **La stratégie porte sur**, sélectionnez une des options d'application de la stratégie suivantes :

   - **Tous les utilisateurs Active Directory** ;
   - **Les utilisateurs Active Directory sélectionnés**.

     L'application suit les actions des utilisateurs sur la base des comptes Active Directory®. La création et la gestion de groupes Active Directory font partie des fonctions de l'administrateur système de l'organisation.

     Pour ajouter ou supprimer des comptes utilisateur soumis à une stratégie, utilisez les boutons  et  .

2. Si vous souhaitez désigner des utilisateurs qui ne seront pas soumis à une stratégie, ajoutez leur compte à la liste **Exclure de la stratégie les utilisateurs suivants**.

   Les exclusions ont toujours priorité en ce qui concerne les autorisations de transfert de fichiers par des utilisateurs. En cas d'ajout d'un compte utilisateur à la liste des exclusions, l'application ne contrôlera jamais les transferts de fichiers vers SharePoint effectués par cet utilisateur.

ÉTAPE 3. SELECTION DES SITES SHAREPOINT A PROTEGER

Cette étape permet de sélectionner les sites Internet de SharePoint sur lesquels l'application doit contrôler le transfert de fichiers.

Cochez manuellement les cases des sites Internet SharePoint qui seront contrôlés ou cliquez sur les boutons **Sélectionner les sous-éléments** et **Annuler la sélection des sous-éléments** afin de cocher les cases automatiquement.

ÉTAPE 4. ACTIONS EN CAS DE VIOLATION D'UNE STRATEGIE

Une *violation de la stratégie* est un événement dans le fonctionnement de l'application lié à une tentative de transfert vers un site SharePoint qui indique une fuite éventuelle de données. L'utilisateur viole la stratégie s'il charge par exemple sur SharePoint des données qui ne lui étaient pas destinées.

Pour configurer les actions de l'application en cas de violation d'une stratégie, procédez comme suit :

1. Cochez la case **Bloquer le transfert de fichiers vers SharePoint**, si vous souhaitez empêcher la fuite de données d'une catégorie.

   Si, lors de l'analyse, l'application détecte dans un fichier plusieurs catégories de données, celui-ci sera bloqué si au moins une des stratégies préconise le blocage des fichiers.

   Si la case est décochée, l'application ne bloque pas le transfert des fichiers vers SharePoint, mais elle crée des incidents en cas de violation d'une stratégie.

2. Dans la liste déroulante **Créer un incident avec priorité**, indiquez le niveau de priorité que l'application doit attribuer aux incidents en cas de violation d'une stratégie.

3. Si nécessaire, cochez la case **Ajouter le fichier aux informations sur l'incident** afin de pouvoir consulter le fichier lors du traitement de l'incident.

4. Si nécessaire, cochez la case **Consigner l'événement dans le journal des événements Windows** afin de conserver les informations sur les violations d'une stratégie de manière centralisée et de pouvoir les utiliser ultérieurement afin de résoudre les erreurs.

   Lorsque un événement relatif à la violation d'une stratégie est consigné dans le journal des événements Windows, le code 16000 lui est attribué. Chaque élément consigné contient le numéro de l'incident et les informations sur l'incident.

5. Dans la liste **Envoyer les notifications par courrier électronique** cochez les cases des collaborateurs qui doivent être informés des violations d'une stratégie. Si vous cochez la case **Avancé**, saisissez les adresses dans le champ en les séparant par une virgule.

   En cas de violation d'une stratégie, l'application enverra des notifications à ces adresses.

6. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

7. Cliquez sur le bouton **OK** pour quitter l'assistant de création d'une stratégie.

La stratégie sera définie pour les catégories de données. Pour consulter la liste des stratégies définies pour une catégorie, cliquez sur le bouton  . Pour réduire la liste des stratégies, cliquez sur le bouton  . Les listes de stratégies sont masquées automatiquement lors du passage à une autre entrée de la Console de gestion.

CONFIGURATION DES ADRESSES DE MESSAGERIE ELECTRONIQUE POUR LA DIFFUSION DES NOTIFICATIONS DE L'APPLICATION

Pour configurer les adresses électroniques en vue de la diffusion des notifications de l'application, procédez comme suit :

1. Ouvrez la Console de gestion.

2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Protection des données contre les fuites**.

3. Dans le groupe **État du module DLP**, cliquez sur le bouton **Configurer**.

   La fenêtre **Adresse électronique** s'ouvre.

4. Saisissez dans le champ les adresses de messagerie auxquelles vous souhaitez envoyer les notifications.

   Si vous renseignez plusieurs adresses, il faut les séparer par un point virgule.

5. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre.

L'application enverra aux adresses indiquées les notifications sur les modifications de l'état du module DLP, sur les erreurs de fonctionnement et sur les incidents et les rapports.

CONFIGURATION DES PARAMETRES DU RAPPORT DETAILLE

Pour configurer les paramètres du rapport détaillé, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Configurez la tâche de rapport détaillé ou de rapport rapide détaillé :
   - Pour configurer une tâche de rapport rapide détaillé existante, choisissez la tâche dans le groupe **Tâches de génération de rapports**, puis cliquez sur le bouton **Modifier**.
   - Pour configurer une tâche de rapport rapide, cliquez sur le bouton **Nouveau rapport** dans le groupe **Visualisation et création de rapports**, puis sélectionnez **Rapport détaillé**.

     La fenêtre des paramètres du rapport s'ouvre.
4. Modifiez les paramètres du rapport.
5. Cliquez sur **OK**.

Vous pouvez configurer les paramètres du rapport détaillé d'une des manières suivantes :

- sélectionner les incidents pour le rapport par stratégies et catégories ;

  Lors de la sélection d'une catégorie, toutes les stratégies définies pour celle-ci sont sélectionnées automatiquement.
- sélectionner pour le rapport les incidents liés à des utilisateurs déterminés ;

  Vous pouvez sélectionner des utilisateurs ou des groupes d'utilisateurs Active Directory, des utilisateurs anonymes ainsi que des utilisateurs sans compte dans Active Directory.
- sélectionner pour le rapport les incidents selon l'état ;
- configurer l'ordre d'affichage des incidents dans le rapport ;

  L'application peut regrouper dans un rapport des incidents contenant des informations similaires selon un ordre que vous définissez.
- sélectionner la période couverte par le rapport ;

  Si vous créez un rapport rapide, vous pouvez désigner n'importe quel intervalle. Si vous configurez une tâche de rapport, la période couverte dépendra de la planification de l'exécution de la tâche. Si vous avez configuré le lancement hebdomadaire de la tâche, le rapport portera sur la semaine antérieure.
- planifier le lancement d'une tâche ;

  L'application génèrera automatiquement les rapports en fonction de la planification. Le cas échéant, vous pouvez désactiver l'exécution automatique d'une tâche.
- Configurer l'envoi automatique du rapport par courrier électronique.

  Le cas échéant, vous pouvez indiquer dans le champ des adresses de messagerie complémentaires en les séparant par un point-virgule. L'application envoie automatiquement le rapport préparé aux adresses indiquées.

CONFIGURATION DES PARAMETRES DU RAPPORT PAR UTILISATEUR

Pour configurer les paramètres du rapport sur les stratégies et les incidents, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Configurez la tâche de rapport par stratégie et par incident ou le rapport rapide par stratégie et par incident :
   - Pour configurer une tâche de rapport par stratégie et par incident existante, sélectionnez-la dans le groupe **Tâches de création de rapports** puis cliquez sur le bouton **Modifier**.
   - Pour configurer un rapport rapide par stratégie et par incident, cliquez sur **Nouveau rapport** dans le groupe **Consultation et création des rapports** puis sélectionnez **Par stratégie et par incident**.

     La fenêtre des paramètres du rapport s'ouvre.
4. Modifiez les paramètres du rapport.
5. Cliquez sur **OK**.

Vous pouvez configurer les paramètres du rapport par utilisateur de la manière suivante :

- Sélectionner les utilisateurs concernés par le rapport ;

  Vous pouvez sélectionner des utilisateurs ou des groupes d'utilisateurs Active Directory, des utilisateurs anonymes ainsi que des utilisateurs sans compte dans Active Directory. Un compte SharePoint (par exemple, `SharePoint\Kaspersky`) peut s'afficher pour les utilisateurs pour lesquels Active Directory n'a pas réussi à définir le compte utilisateur.
- Sélectionner les incidents pour le rapport par catégorie ;

  Le nombre de violations pour des catégories de données sélectionnées est affiché pour chaque utilisateur.
- Sélectionner les incidents pour le rapport par état ;
- Configurer l'ordre d'affichage des informations sur les utilisateurs dans le rapport ;

  L'application peut regrouper les informations sur des utilisateurs associés aux mêmes violations dans l'ordre que vous indiquez.
- sélectionner la période couverte par le rapport ;

  Si vous créez un rapport rapide, vous pouvez indiquer n'importe quel intervalle de temps. Si vous configurez une tâche de rapport, la période couverte par celui-ci dépend de la planification du lancement de la tâche. Si vous avez configuré le lancement hebdomadaire de la tâche, le rapport portera sur la semaine antérieure.
- planifier le lancement d'une tâche ;

  L'application génèrera automatiquement les rapports en fonction de la planification. Le cas échéant, vous pouvez désactiver l'exécution automatique d'une tâche.
- Configurer l'envoi automatique du rapport par courrier électronique.

  Le cas échéant, vous pouvez indiquer dans le champ des adresses de messagerie complémentaires en les séparant par un point-virgule. L'application enverra le rapport créé aux adresses indiquées.

CONFIGURATION DES PARAMETRES DU RAPPORT SUR LES KPI DU SYSTEME

Pour configurer les paramètres du rapport sur les KPI du système, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Configurez la tâche du rapport sur les KPI du système ou la tâche de rapport rapide sur les KPI du système :
   - Pour configurer une tâche existante de rapport sur les KPI du système, sélectionnez la tâche dans le groupe **Tâches de génération de rapports**, puis cliquez sur le bouton **Modifier**.
   - Pour configurer une tâche de rapport rapide sur les KPI du système, cliquez sur le bouton **Nouveau rapport** dans le groupe **Visualisation et création de rapports**, puis sélectionnez **KPI du système**.

     La fenêtre des paramètres du rapport s'ouvre.
4. Modifiez les paramètres du rapport.
5. Cliquez sur **OK**.

Vous pouvez configurer les paramètres du rapport sur les KPI du système d'une des manières suivantes :

- sélectionner la période couverte par le rapport ;

  Si vous créez un rapport manuellement, vous pouvez désigner n'importe quel intervalle. Si le rapport est généré automatiquement, la période couverte dépendra de la planification de l'exécution de la tâche. Si vous avez configuré le lancement hebdomadaire de la tâche, le rapport portera sur la semaine antérieure.

- planifier le lancement d'une tâche ;

  L'application génèrera automatiquement les rapports en fonction de la planification. Le cas échéant, vous pouvez désactiver l'exécution automatique d'une tâche.

- Configurer l'envoi automatique du rapport par courrier électronique.

  Le cas échéant, vous pouvez indiquer dans le champ des adresses de messagerie complémentaires en les séparant par un point-virgule.

CONFIGURATION DES PARAMETRES DU RAPPORT PAR STRATEGIE ET PAR INCIDENT

Pour configurer les paramètres du rapport sur les stratégies et les incidents, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Configurez la tâche de rapport par stratégie et par incident ou le rapport rapide par stratégie et par incident :
   - Pour configurer une tâche de rapport par stratégie et par incident existante, sélectionnez-la dans le groupe **Tâches de création de rapports** puis cliquez sur le bouton **Modifier**.

- Pour configurer un rapport rapide par stratégie et par incident, cliquez sur **Nouveau rapport** dans le groupe **Consultation et création des rapports** puis sélectionnez **Par stratégie et par incident**.

  La fenêtre des paramètres du rapport s'ouvre.

4. Modifiez les paramètres du rapport.

5. Cliquez sur **OK**.

Vous pouvez configurer les paramètres du rapport par stratégie et par incident de la manière suivante :

- Sélectionner les incidents pour le rapport par catégorie ;

  L'application sélectionne pour le rapport les incidents dont l'état est *Fermé*. Les incidents dont l'état est différent ne sont pas inclus dans le rapport. Pour chaque incident lié à la catégorie sélectionnée, le rapport indique la stratégie et la raison de la fermeture de l'incident.

- sélectionner la période couverte par le rapport ;

  Si vous créez un rapport rapide, vous pouvez désigner n'importe quel intervalle. Si vous configurez une tâche de rapport, la période couverte dépend de la planification du lancement de la tâche. Si vous avez configuré le lancement hebdomadaire de la tâche, le rapport portera sur la semaine antérieure.

- planifier le lancement d'une tâche ;

  L'application génèrera automatiquement les rapports en fonction de la planification. Le cas échéant, vous pouvez désactiver l'exécution automatique d'une tâche.

- Configurer l'envoi automatique du rapport par courrier électronique.

  Le cas échéant, vous pouvez indiquer dans le champ des adresses de messagerie complémentaires en les séparant par un point-virgule. L'application enverra le rapport créé aux adresses indiquées.

CONFIGURATION DU NIVEAU DE CORRESPONDANCE

Le *niveau de correspondance* désigne la quantité de cellules dans le tableau qui correspondent au contenu que l'application recherche sur SharePoint. Le nombre de cellules utilisées pour la recherche est défini par les croisements uniques des colonnes et des lignes du tableau. Le niveau de correspondance possède deux paramètres :

- **Valeur seuil de lignes**. Nombre minimal de lignes dont les données sont recherchées par l'application sur SharePoint.

- **Valeur seuil de colonnes**. Nombre minimal de colonnes dont les données sont recherchées par l'application sur SharePoint.

La correspondance avec les données du tableau donne un fichier qui contient les données du nombre indiqué de colonnes sur le nombre indiqué de lignes. Il n'est pas nécessaire que les même colonnes correspondent dans différentes lignes.

Exemple :

Un tableau au format CSV contenant les données suivantes a été ajouté à la catégorie :

COLONNE1	COLONNE2	COLONNE3	COLONNE4	COLONNE5
1946	2718	0	0	0
3376	2753	58	1	4
3370	2746	67	9	4
3373	2731	6	1	7

Le niveau de correspondance suivant avec les données du tableau a été défini : valeur seuil de lignes : 2, valeur seuil de colonnes : 3.

L'application trouve les fichiers dont les données correspondent à six cellules de données. Les données correspondantes doit se trouver simultanément dans deux lignes minimum et dans chaque ligne, elles doivent correspondre avec trois cellules minimum. Par exemple :

COLONNE1	COLONNE2	COLONNE3	COLONNE4	COLONNE5
1946	2718	0	0	0
3376	2753	58	1	4
3370	2746	67	9	4
3373	2731	6	1	7

Dans ce niveau de correspondance défini, l'application recherche également le fichier qui contient les données suivantes :

COLONNE1	COLONNE2	COLONNE3	COLONNE4	COLONNE5
1946	2718	0	0	0
3376	2753	58	1	4
3370	2746	67	9	4
3373	2731	6	1	7

Les fichiers qui contiennent un nombre de correspondances inférieur seront ignorés par l'application. Par exemple :

COLONNE1	COLONNE2	COLONNE3	COLONNE4	COLONNE5
1946	2718	0	0	0
3376	2753	58	1	4
3370	2746	67	9	4
3373	2731	6	1	7

Dans l'exemple fourni, les données de trois cellules correspondent au tableau au format CSV dans une ligne seulement. Le fichier ne respecte pas le valeur de seuil de lignes (2) et il sera ignoré par l'application.

MISE A JOUR DE LA LISTE DES INCIDENTS

La liste des incidents n'est pas mise à jour automatiquement. Il faut actualiser la liste manuellement pour pouvoir traiter les nouveaux incidents.

Pour actualiser la liste des incidents, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Dans le panneau de résultats de l'entrée, cliquez sur le bouton **Mettre à jour**.

L'application ajoute à la liste les incidents créés depuis la dernière mise à jour de la liste.

RECHERCHE DES INCIDENTS A L'AIDE D'UN FILTRE

La liste des incidents permet d'afficher la liste des incidents, peu importe l'heure de création ou leur état actuel. Vous pouvez filtrer la liste des incidents de telle sorte qu'elle affiche uniquement les incidents correspondant à un état donné ou les incidents survenus pendant la période indiquée.

Pour trouver les incidents à l'aide d'un filtre, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Le groupe **Filtre des incidents** permet de configurer la condition de filtrage des incidents.

   Chaque condition de filtrage possède deux paramètres : le critère et la valeur. La liste déroulante de gauche permet de sélectionner les critères de filtrage des incidents. Les informations relatives à un incident servent de critères de filtrage. La liste déroulante qui se trouve à côté permet de définir la valeur du critère sélectionné et selon laquelle le filtrage va être réalisé. L'aspect de la liste déroulante dépend du critère de filtrage sélectionné.
4. Le cas échéant, vous pouvez ajouter des conditions de filtrage en cliquant sur le bouton **Ajouter une condition**.

   L'application filtre les données selon toutes les conditions ajoutées au filtre des incidents.
5. Cliquez sur le bouton **Appliquer le filtre** pour rechercher des incidents.

Le groupe **Liste des incidents** affiche les incidents qui satisfont aux conditions du filtre.

RECHERCHE DES STRATEGIES PAR UTILISATEUR

Pour trouver des stratégies définies par rapport à certains utilisateurs, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Dans le groupe **Recherche de stratégies**, sélectionnez une des options de recherche suivantes :

   - **Par utilisateur absent d'Active Directory**, si vous cherchez des stratégies établies en lien avec des utilisateurs anonymes ou dont les comptes sont absents d'Active Directory ;
   - **Par utilisateur sélectionné**, si vous cherchez des stratégies établies en lien avec des utilisateurs définis, dont les comptes figurent dans Active Directory.

     Le bouton **Sélectionner** vous permet d'indiquer le compte d'un utilisateur pour la recherche de stratégies. Il est impossible de sélectionner plusieurs comptes.
4. Cliquez sur le bouton **Rechercher** pour lancer la recherche de stratégies.

L'application affichera la liste des stratégies trouvées. Pour chaque stratégie, sont affichées la catégorie de données et l'action de l'application en cas de violation de cette stratégie. Si la stratégie n'est pas active, cela sera indiqué dans la colonne **Action**.

CONSULTATION DES DETAILS D'UN INCIDENT

Pour consulter les détails d'un incident, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Dans la liste, sélectionnez l'incident dont vous souhaitez consulter les détails.

4. Cliquez sur le bouton **Visualiser**.

   La fenêtre **Caractéristiques de l'incident** s'ouvre. La fenêtre permet de consulter les détails de l'incident et de modifier l'état de celui-ci. Vous pouvez naviguer entre les incidents de la liste à l'aide des boutons **Suivant** et **Précédent**.

   L'onglet **Parcourir** affiche les détails de l'incident et ses origines.

   L'onglet **Historique** affiche les informations sur l'historique du traitement de l'incident (par exemple, la modification de l'état de l'incident ou son archivage).

5. Cliquez sur le bouton **Annuler** pour quitter la consultation des détails de l'incident.

Si vous aviez modifié l'état d'un incident pendant la consultation de ses détails, cliquez sur **OK** pour enregistrer les modifications.

CONSULTATION D'UN RAPPORT DETAILLE

Pour consulter un rapport détaillé, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport pour lequel le type **Détaillé** figure dans la colonne **Type de rapport**.
4. Cliquez sur le bouton **Visualiser**.

Le rapport s'ouvre dans le navigateur installé par défaut.

Le rapport contient les informations suivantes :

- Paramètres du rapport :
  - type de rapport ;
  - date et heure de génération du rapport ;
  - nombre d'incidents sélectionnés pour le rapport ;
  - période du rapport ;
  - états utilisés par l'application pour sélectionner les incidents en vue du rapport ;
  - utilisateurs selon lesquels l'application a sélectionné les incidents en vue du rapport ;
  - catégories et stratégies utilisées par l'application pour sélectionner les incidents en vue du rapport.
- Liste des incidents sélectionnés pour le rapport.

  La liste des incidents contient un tableau avec les détails de chaque incident repris dans le rapport. Les incidents du tableau sont classés selon les informations relatives à l'incident sélectionnées dans les paramètres du rapport.

CONSULTATION DU RAPPORT SUR LES KPI DU SYSTEME

Pour visualiser le rapport sur les KPI du système, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport pour lequel le type **KPI du système** est affiché dans la colonne **Type**.
4. Cliquez sur le bouton **Visualiser**.

Le rapport s'ouvre dans le navigateur installé par défaut.

Le rapport contient les informations suivantes :

- Paramètres du rapport :
  - type de rapport ;
  - date et heure de génération du rapport ;
  - période du rapport.
- Données sur les indices d'efficacité :
  - **Dans la zone d'application des stratégies**. Nombre de fichiers dont les données ont été analysées par l'application.
  - **Sains**. Nombre de fichiers ne contenant aucune donnée correspondant aux catégories.
  - **Violations**. Nombre de fichiers contenant des données correspondant aux catégories.
  - **Erreurs**. Nombre de fichiers dont les données n'ont pas été vérifiées suite à des erreurs (par exemple, pas d'accès aux données de l'utilisateur).
  - **Temps d'attente de l'analyse**. Nombre de fichiers dont les données n'ont pas été vérifiées suite à un dépassement du délai accordé à la vérification.
  - **Hors de la zone d'application des stratégies**. Nombre de fichiers dont les données n'ont pas été vérifiées car les utilisateurs ou les sites SharePoint associés à ces derniers ne figuraient pas dans les paramètres de la stratégie.
  - **Total**. Nombre de fichiers traités au cours de la période indiquée.
- Données sur les violations :
  - Liste des catégories dont les stratégies ont été violées au cours de la période couverte par le rapport. Le nombre et le rapport de violations par catégorie sur l'ensemble des violations (en pour cent) sont affichés pour chaque catégorie.
  - **Total**. Total des violations sur l'ensemble des catégories.

CONSULTATION DU RAPPORT SUR LES UTILISATEURS

Pour visualiser le rapport sur les utilisateurs, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.

3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport pour lequel le type **Par utilisateur** est affiché dans la colonne **Type de rapport**.

4. Cliquez sur le bouton **Visualiser**.

Le rapport s'ouvre dans le navigateur installé par défaut.

Le rapport contient les informations suivantes :

- Paramètres du rapport :
  - type de rapport ;
  - date et heure de génération du rapport ;
  - nombre d'incidents sélectionnés pour le rapport ;
  - période du rapport ;
  - états utilisés par l'application pour sélectionner les incidents en vue du rapport ;
  - utilisateurs selon lesquels l'application a sélectionné les incidents en vue du rapport ;
  - catégories et stratégies utilisées par l'application pour sélectionner les incidents en vue du rapport.
- Tableau des incidents.

  Le tableau **Nombre d'incidents par catégorie chez les utilisateurs** contient la liste des incidents sélectionnés pour le rapport. Pour chaque utilisateur, le service auquel il appartient, le nombre d'incidents associés à sa personne et les noms des catégories auxquelles appartiennent ces incidents sont affichés.

Pour consulter le rapport sur les stratégies et les incidents, procédez comme suit :

1. Ouvrez la Console de gestion.

2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.

3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport pour lequel le type **Par stratégie et par incident** est affiché dans la colonne **Type de rapport**.

4. Cliquez sur le bouton **Visualiser**.

Le rapport s'ouvre dans le navigateur installé par défaut.

Le rapport contient les informations suivantes :

- Paramètres du rapport :
  - type de rapport ;
  - date et heure de génération du rapport ;
  - nombre d'incidents sélectionnés pour le rapport ;
  - période du rapport ;
  - catégories utilisées par l'application pour sélectionner les incidents en vue du rapport ;
- Tableau des incidents.

  Le tableau **Nombre d'incidents par stratégie** contient la liste des incidents sélectionnés pour le rapport. Pour chaque catégorie, les stratégies définies sont affichées. Chaque stratégie est accompagnée du nombre d'incidents créés lors des violations de cette stratégie et des états de tous les incidents à l'heure actuelle.

CONSULTATION DES RESULTATS DE LA RECHERCHE

Pour consulter les résultats de la recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans la liste des rapports du groupe **Résultats de la recherche**, sélectionnez le rapports à consulter, puis cliquez sur **Visualiser**.

Le rapport s'ouvre dans l'éditeur de texte installé par défaut.

Le rapport contient les informations suivantes sur les résultats de la recherche :

- Paramètres de la tâche :
  - sites SharePoint sur lesquels la recherche est effectuée ;

    Si l'accès aux sites SharePoint repris dans les paramètres de la recherche n'est pas disponible, le rapport indiquera seulement l'adresse et les informations relatives à l'erreur par faute d'accès.

  - catégorie selon laquelle la recherche a été exécutée ;
  - raisons de la fin de l'opération (par exemple, la tâche a été arrêtée manuellement).
- données relatives au début et à la fin de la recherche ;
- Nombre de fichiers analysés ;
- Liste des fichiers qui satisfont aux critères de la recherche. Les informations suivantes sont proposées pour chaque fichier :
  - nom et format du fichier ;
  - chemin d'accès complet au fichier sur le site de SharePoint ;
  - version du fichier ;
  - nom de l'utilisateur qui a transmis le fichier sur SharePoint (première version du fichier) ;
  - nom de l'utilisateur qui a modifié le fichier (dernière version du fichier) ;
  - date et heure du début de l'analyse du fichier ;
  - nom des catégories de données détectées dans le fichier.

    Si un fichier contenait les données de plusieurs catégories, les informations relatives à chaque catégorie détectée seront affichées dans une colonne distincte du tableau.

    Si le fichier contenait une catégorie de données tabulaires, le rapport affichera le nombre de lignes du fichier CSV chargé dans la catégorie.
- Informations relatives à d'éventuelles erreurs :
  - fichier inaccessible ;
  - impossible d'ouvrir le fichier ;
  - impossible d'analyser le fichier.

CONSULTATION DES INFORMATIONS SUR L'ETAT DE LA PROTECTION

Les informations sur l'état de la protection des données apparaissent dans la zone de travail de l'entrée **Protection des données contre les fuites** de la console de gestion.

Le groupe **État du module DLP** affiche les informations relatives à l'état actuel du module et les messages relatifs aux erreurs dans son fonctionnement :

- *Activé*. L'administrateur de Kaspersky Security a activé le module DLP et l'application fonctionne correctement sur tous les serveurs.
- *Activé, fonctionne avec des erreurs*. L'administrateur Kaspersky Security a activé le module DLP, mais des erreurs sont survenues pendant le fonctionnement de l'application. L'application affiche les informations relatives aux erreurs dans la partie inférieure du groupe. Pour chaque type d'erreur, l'application affiche le nom du serveur sur lequel l'erreur a été découverte. Vous avez le choix entre les types d'erreur suivants :
  - *Erreurs d'analyse*. L'application ne parvient pas à analyser les fichiers en raison du dépassement du délai d'attente, d'erreurs d'infrastructure ou d'erreurs de l'intercepteur.
  - *Erreur de licence du module DLP*. L'application ne parvient pas à analyser les fichiers en raison de l'absence de licence du module DLP, de l'expiration de la licence ou de l'ajout du fichier clé à la liste noire.
  - *Serveur inaccessible.* L'application ne peut analyse les fichiers en raison de l'inaccessibilité du serveur SharePoint (le serveur a peut-être été éteint par l'administrateur).
- *Désactivé*. L'administrateur a désactivé le module DLP. L'application n'analyse pas les fichiers envoyés par les utilisateurs sur SharePoint.

Le groupe **Incidents ouverts** reprend les informations suivantes sur les utilisateurs et les incidents ouverts actuellement :

- nombre d'utilisateurs uniques auxquels les incidents ouverts sont associés ;
- classement des utilisateurs comptant le plus de violations des stratégies ;
- nombre d'incidents portant l'état *Nouveau* ;
- nombre d'incidents portant l'état *En cours de traitement* ;

Un diagramme représente les données de la relation entre les incidents portant l'état *Nouveau* et les incidents portant l'état *En cours de traitement*. Le diagramme reprend les statistiques par incidents liés aux catégories de données sélectionnées. Vous pouvez modifier la liste des catégories selon lesquelles s'affichent les statistiques (cf. section « Sélection des catégories pour la génération des statistiques par incident » à la page 24).

Le groupe **Statistiques** permet de consulter les informations relatives aux fichiers analysés et aux incidents fermés sur une période de 7 ou de 30 jours. Les informations suivantes sont fournies en fonction de la période sélectionnée :

- nombre de fichiers transmis par les utilisateurs sur SharePoint ;
- nombre de fichiers analysés par l'application ;
- nombre d'incidents créés ;
- nombre de fichiers non analysés en raison du dépassement du délai d'attente ;
- nombre de fichiers non analysés en raison d'une erreur ;

Les données relatives aux raisons de la fermeture des incidents sont présentées sous la forme d'un diagramme. Le diagramme reprend les statistiques par incidents liés aux catégories de données sélectionnées. Vous pouvez modifier la liste des catégories selon lesquelles s'affichent les statistiques (cf. section « Sélection des catégories pour la génération des statistiques par incident » à la page 24).

GENERATION D'UN RAPPORT RAPIDE

Pour créer un rapport rapide, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans le groupe **Consultation et création des rapports**, cliquez sur le bouton **Nouveau rapport**.
4. Sélectionnez le type de rapport à créer dans la liste déroulante.
5. Configurez les paramètres de création d'un rapport dans la fenêtre qui s'ouvre.
6. Cliquez sur **OK** pour lancer la création d'un rapport.

Le rapport prêt apparaît dans la liste des rapports du groupe **Consultation et création des rapports** et il s'ouvre automatiquement dans une fenêtre du navigateur.

ENREGISTREMENT DES RAPPORTS

Pour enregistrer un rapport, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport à enregistrer, puis cliquez sur **Enregistrer**.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au dossier d'enregistrement du rapport, puis cliquez sur **Enregistrer**.

L'application enregistre le rapport dans le fichier au format HTML dans le dossier indiqué. Par défaut, le nom du fichier enregistré correspond au nom du rapport.

ENREGISTREMENT DES RESULTATS DE LA RECHERCHE

Pour enregistrer les résultats de la recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans la liste des rapports du groupe **Résultats de la recherche**, sélectionnez le rapport, puis cliquez sur **Enregistrer**.

L'application enregistre le rapport au format CSV dans le dossier que vous avez indiqué.

SUPPRESSION DES INCIDENTS ARCHIVES

Pour supprimer des incidents archivés, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Incidents**.
3. Cliquez sur le bouton **Supprimer les archivés** situé sous la liste des incidents.

Une fois que la demande de suppression aura été confirmée, l'application supprimera les incidents portant l'état *Archivé* dans la liste des incidents.

SUPPRESSION D'UNE TACHE

Pour supprimer une tâche de recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans la liste des tâches du groupe **Tâches de recherche**, sélectionnez la tâche à supprimer, puis cliquez sur **Supprimer**.

Une fois que la demande de suppression aura été confirmée, l'application supprimera la tâche sans possibilité de la restaurer.

SUPPRESSION D'UNE CATEGORIE

Pour supprimer une catégorie, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Dans la liste des catégories, sélectionnez la catégorie que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.

Une fois que la demande de suppression aura été confirmée, l'application supprimera la catégorie sans possibilité de la restaurer.

Si des stratégies avaient été définies pour la catégorie, elles seront supprimées en même temps.

Si la catégorie supprimée intervenait dans des tâches de recherche, les paramètres de la tâche seront modifiés après la suppression.

SUPPRESSION DU RAPPORT

Pour supprimer un rapport, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Rapports**.
3. Dans la liste des rapports qui figure dans le groupe **Consultation et création des rapports**, sélectionnez le rapport à supprimer, puis cliquez sur **Supprimer**.

   Vous pouvez supprimer plusieurs rapports à la fois.

Une fois que la demande de suppression aura été confirmée, l'application supprimera les rapports sélectionnés sans possibilité de les restaurer.

SUPPRESSION D'UNE STRATEGIE

Pour supprimer une stratégie, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console de gestion, sélectionnez l'entrée **Catégories et stratégies**.
3. Dans le groupe **Catégories**, sélectionnez la catégorie de données confidentielles dont vous souhaitez supprimer la stratégie, puis cliquez sur le bouton .

   La liste des stratégies définies pour la catégorie apparaît.
4. Sélectionnez dans la liste la stratégie que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.
5. Confirmez la suppression de la stratégie dans la boîte de dialogue.

L'application supprime la stratégie sans possibilité de restauration.

SUPPRESSION DES RESULTATS DE LA RECHERCHE

Pour supprimer les résultats de la recherche, procédez comme suit :

1. Ouvrez la Console de gestion.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche**.
3. Dans la liste des rapports du groupe **Résultats de la recherche**, sélectionnez le rapport à supprimer, puis cliquez sur **Supprimer**.

Une fois que la demande de suppression aura été confirmée, l'application supprimera les rapports sur les résultats de la recherche sans possibilité de la restaurer.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia en 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

PRODUITS. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des applications antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que pour tablettes, smartphones et autres appareils nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions en combinaison avec des outils d'administration centralisée permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et ils sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases Anti-Spam* sont actualisées *toutes les 5 minutes*.

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment Safenet SafeNet (E-U), Alt-N Technologies (E-U), Blue Coat Systems (E-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (E-U), Openwave Messaging (Irlande), D-Link (Taïwan), M86 Security (E-U), GFI Software (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), Netasq+Arkoon (France), NETGEAR (E-U), Parallels (E-U), SonicWALL (E-U), WatchGuard Technologies (E-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab,c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie Virus :	http://www.securelist.com/fr/
Laboratoire d'étude des virus :	newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt qui se trouve dans le dossier d'installation de l'application.

AVIS SUR LES MARQUES

Les marques commerciales et les marques de service enregistrées appartiennent à leurs propriétaires respectifs.

Active Directory, Excel, SharePoint, SQL Server et Windows sont des marques déposées de Microsoft Corporation enregistrées aux Etats-Unis et dans d'autres pays.