Kaspersky Security 9.0 for Microsoft Exchange Servers

Manuel de l'expert en sécurité 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.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et à titre d'information.

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.

Kaspersky Lab ne pourra être tenue responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Date d'édition : 10/10/2014

© 2014 Kaspersky Lab ZAO. Tous droits réservés.

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

TABLE DES MATIERES

PRESENTATION DU MANUEL

Le présent document constitue le manuel de l'expert en sécurité de l'information de Kaspersky Security 9.0 for Microsoft® Exchange Servers (ci-après, Kaspersky Security).

Le manuel vise les objectifs suivants :

- Aider à utiliser l'application.
- Offrir un accès rapide aux informations pour répondre aux questions liées au fonctionnement de Kaspersky Security.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

Kaspersky Security 9.0 for Microsoft Exchange Servers (cf. page 8)

Cette section décrit brièvement les possibilités de l'application.

Interface de l'application (cf. page 14)

Cette section contient des informations sur les principaux éléments de l'interface graphique de l'application : la fenêtre principale de la Console de gestion, arborescence de la Console de gestion, espaces de travail.

Lancement et arrêt de l'application (cf. page 15)

Cette section explique comment lancer et arrêter l'application.

État de la protection des données contre les fuites (cf.page 16)

Cette section contient des informations sur l'état par défaut de la protection des données contre les fuites ainsi que des instructions pour obtenir des informations sur l'état du Module DLP et des statistiques concernant le fonctionnement de ce module.

Configuration des adresses des experts en sécurité de l'information (cf. page 19)

Cette section explique comment configurer les adresses des experts en sécurité de l'information, de préférence avant de commencer à utiliser l'application.

Utilisation des catégories (cf. page 20)

Cette section contient des instructions pour la création, la modification et la suppression des catégories DLP.

Utilisation des stratégies (cf. page 24)

Cette section contient des instructions sur la création, la modification et la suppression des stratégies DLP.

Utilisation des incidents (cf. page 32)

Cette section contient des instructions sur le traitement des incidents créés.

Utilisation des rapports

Cette section contient des informations relatives aux rapports sur le fonctionnement du module DLP, des instructions sur la création, la consultation, l'enregistrement et la suppression de rapports ainsi que sur la création, la modification, l'exécution et la suppression des tâches de création de rapports.

Kaspersky Lab ZAO (cf. page 56)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (cf. page 57)

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

Avis sur les marques (cf. page 58)

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

CONVENTIONS

Le présent document respecte des conventions (cf. tableau ci-dessous).

Таблица 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
La *mise à jour*, c'est ... L'événement *Les bases sont obsolètes* survient.	Les éléments de texte 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. Ces touches doivent être enfoncées simultanément.
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 : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir à l'aide du clavier.
<Nom de l'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable, sans les chevrons.

KASPERSKY SECURITY 9.0 FOR MICROSOFT EXCHANGE SERVERS

Kaspersky Security 9.0 for Microsoft Exchange Servers est une application qui a été développée pour assurer la protection des serveurs de messagerie tournant sous Microsoft Exchange Server contre les virus, les chevaux de Troie, les vers et autres types de menaces pouvant être diffusées par courrier électronique, ainsi que contre le spam, le phishing et les fuites non préméditées d'informations confidentielles appartenant à la société par le biais de courriers électroniques.

Kaspersky Security 9.0 for Microsoft Exchange Servers contient un module de lutte contre les fuites de données (Data Loss Prevention, DLP) : le *Module DLP*. Le module DLP recherche la présence éventuelle d'informations confidentielles ou d'informations répondant à des caractéristiques précises comme des données de carte de crédit ou des données financières ou personnelles d'employés d'une entreprise dans le courrier. Si le Module DLP détecte ce genre d'informations dans le message, il consigne dans son journal une entrée sur la violation de la sécurité des données (*incident*). Ces entrées permettront d'identifier plus tard qui a tenté d'envoyer ces informations et le destinataire. Le module DLP permet de bloquer la transmission de messages contenant des données confidentielles ou d'autoriser l'envoi de tels messages, avec simplement consignation dans le journal.

Le module DLP tire ses conclusions sur la violation de la sécurité des données sur la base des *catégories DLP* et *des stratégies DLP*.

Si la législation en vigueur dans votre pays impose la notification des citoyens sur le contrôle de leur activité dans les réseaux de transmission de données, il vous faudra informer les utilisateurs sur le fonctionnement du Module DLP.

Des informations supplémentaires concernant d'autres fonctions de l'application sont disponibles dans le *Manuel de l'administrateur de Kaspersky Security 9.0 for Microsoft Exchange Servers*.

DANS CETTE SECTION

PRESENTATION DES CATEGORIES DLP

Les catégories DLP (ci-après, « les catégories ») sont des modèles de données selon lesquels le Module DLP recherche les fuites de données dans un message. Les catégories sont réparties entre les catégories de Kaspersky Lab et les catégories utilisateur. Les catégories de Kaspersky Lab sont préparées par les experts de Kaspersky Lab et sont fournies avec l'application et actualisées lors de la mise à jour des bases de l'application. Les catégories définies par l'utilisateur peuvent être créées de manière indépendante.

Catégories définies par l'utilisateur

- **Catégorie de données tabulaires**

  Ce type de catégorie se présente sous la forme d'une empreinte numérique de données sous forme de tableau. Par exemple, il peut s'agir de tableaux de données personnelles sur des employés et des clients reçus via les systèmes de GRC (cf. section « Création et modification d'une catégorie de données tabulaires » à la page 20). Une recherche à l'aide de cette catégorie permet d'identifier parmi les données protégées des combinaisons de cellules comprenant un nombre défini de lignes et de colonnes (cf. section « Exemple d'une catégorie de données tabulaires » à la page 21).

- **Catégorie de mots clés**

  Ce type de catégorie se présente sous la forme d'un mot-clé ou d'une expression composée de mots-clés à l'aide de fonctions spécifiques (cf. section « Création et modification de la catégorie de mots-clés » à la page 21). La recherche selon cette catégorie permet de trouver dans les données protégées une combinaison de mots ou d'expression qui répondent aux conditions de recherche complexes, par exemple, la présence de deux mots séparés par un nombre de mots définis. La catégorie des mots clés permet de protéger les documents contenant des termes spécifiques (par exemple, noms de nouvelles technologies ou de nouveaux produits qui constituent un secret commercial) contre la fuite de données.

Les nouvelles catégories et modifications d'utilisateurs créées dans les catégories d'utilisateurs s'étendent à tous les Serveurs de sécurité dotés du Module DLP dans les 30 minutes qui suivent.

Catégories de Kaspersky Lab

- **Documents administratif (Russie)**

  Cette catégorie permet de protéger les principaux documents administratifs et réglementaires de l'activité économique en Russie comme les commandes ou les instructions.

- **Documents confidentiels (Russie)**

  Cette catégorie permet de protéger les documents de l'activité économique en Russie réservés à un cercle restreint de personnes. Il s'agit par exemple de documents portant la note « Usage interne uniquement » ou « Informations confidentielles ».

- **Documents financiers (Russie)**

  Cette catégorie permet de protéger les documents financiers standard utilisés dans les entreprises russes comme les factures, les contrats.

- **Données médicales (Russie)**

  Cette catégorie permet de protéger les données médicales personnelles des citoyens de Russie.

- **Données médicales (Allemagne)**

  Cette catégorie permet de protéger les données médicales personnelles des citoyens d'Allemagne.

- **Données médicales (Grande-Bretagne)**

  Cette catégorie permet de protéger les données médicales personnelles des citoyens de Grande-Bretagne.

- **Données médicales (Etats-Unis)**

  Cette catégorie permet de protéger les données médicales personnelles des citoyens des Etats-Unis.

- **Cartes de paiement**

  Cette catégorie permet de protéger les données confidentielles conformément à la norme PCI DSS (Payment Card Industry Data Security Standard), la norme internationale adoptée pour garantir la sécurité des données du secteur des cartes de paiement. Elle permet d'identifier dans les données protégées les informations relatives aux cartes de paiement comme le numéro de la carte (avec ou sans trait d'union, avec ou sans le code CVV) et les dumps de la bande magnétique. A l'aide de la catégorie « Cartes de paiement », vous pouvez

protéger les données personnelles des détenteurs de cartes de paiement contre toute utilisation ou diffusion non autorisée.

- **Données personnelles (Allemagne)**

  Cette catégorie permet de protéger les données personnelles conformément aux dispositions de la législation allemande.

- **Données personnelles (Russie)**

  Cette catégorie permet de protéger les données personnelles conformément aux dispositions de la législation russe.

- **Données personnelles (Grande-Bretagne)**

  Cette catégorie permet de protéger les données personnelles conformément aux dispositions de la législation britannique.

- **Données personnelles (Etats-Unis)**

  Cette catégorie permet de protéger les données personnelles conformément aux dispositions de la législation américaine. La catégorie permet d'identifier dans les données protégées toute information qui permet d'identifier un citoyen ou son emplacement comme les données du passeport ou du permis de conduire, les informations de contribuable ou les numéros de sécurité sociale.

- **Loi fédérale N152 (Russie)**

  Cette catégorie permet de protéger les données personnelles couvertes par la loi fédérale 152 de la Fédération de Russie. Cette catégorie regroupe les catégories « Données personnelles (Russie) » et « Données médicales (Russie) ».

- **Loi fédérale HIPAA (Etats-Unis)**

  Cette catégorie permet de protéger les données personnelles relatives à la santé et couvertes par la loi fédérale HIPAA des Etats-Unis.

La liste des catégories de Kaspersky Lab livrées avec l'application peut différer de la liste citée. De plus, cette sélection peut être enrichie lors de la mise à jour de la base de données de l'application.

PRESENTATION DES STRATEGIES DLP

Il est possible d'établir des stratégies DLP (ci-après, *stratégies*) en se basant sur les catégories de Kaspersky Lab et sur les catégories DLP définies par l'utilisateur (cf. section « Création d'une stratégie » à la page 24).

La zone d'action d'une stratégie comprend :

- Le nombre d'expéditeurs dont les messages doivent être analysés par l'application conformément à cette stratégie.

- Le nombre de destinataires dont les messages doivent être analysés par l'application conformément à cette stratégie.

L'application applique les stratégies aux messages sortants qui entrent dans la zone d'action des stratégies et recherche la présence éventuelle de données confidentielles qui correspondent aux catégories de ces stratégies.

La stratégie détermine également les actions. L'application exécute ces actions sur les messages dans lesquels ont été détectées des données confidentielles.

Une catégorie peut servir à la création de plusieurs stratégies aux zones d'action différentes et avec des actions différentes à exécuter.

Les nouvelles stratégies et modifications créées dans les stratégies s'étendent à tous les Serveurs de sécurité dotés du Module DLP dans les 30 minutes qui suivent.

PRESENTATION DES INCIDENTS

Si le contenu du message correspond à des données de la catégorie et à l'ensemble des conditions définies dans la stratégie, le module DLP crée un incident qui évoque la violation de cette stratégie. Si un même message de courrier électronique viole plusieurs stratégies de sécurité de l'information simultanément, le Module DLP crée autant d'incidents qu'il y a de stratégies violées (cf. section « Processus d'analyse des messages par le Module DLP » à la page 12).

Chaque incident contient des informations sur l'objet de l'incident (le message à l'origine de la violation de la sécurité de l'information), sur l'expéditeur et les destinataires du message, sur la stratégie violée, ainsi que des informations techniques telles que l'identifiant de l'incident ou l'heure de création de l'incident (cf. section « Consultation de la liste des incidents » à la page 32).

Chaque incident doit être traité par un expert en sécurité de l'information. Le traitement de l'incident inclut la consignation de la violation et l'adoption des mesures techniques et organisationnelles à prendre pour renforcer la protection des données confidentielles.

Etat de l'incident

L'état de l'incident indique l'état de son traitement. Un incident qui vient d'être créé possède l'état *Nouveau*. Lors du traitement d'un incident, l'expert en sécurité de l'information change son état. Le traitement de l'incident est terminé lorsque l'expert en sécurité de l'information lui attribue un des états *Clos (<raison>)*. Les états *Nouveau* et *En traitement* sont des états *ouverts*, et les états *Clos (<raison>)* sont des états *fermés*.

Таблица 2. États des incidents

ETAT	TYPE	VALEUR
Nouveau	Ouvert	Nouvel incident. Le traitement de l'incident n'a pas encore débuté.
En traitement	Ouvert	L'enquête sur l'incident est en cours.
Clos (traité)	Fermé	L'incident a été traité et les mesures requises ont été adoptées.
Clos (faux positif)	Fermé	La stratégie a été violée, mais l'envoi de données protégée était un faux positif. Il n'y a pas eu de violation de la sécurité des informations. Il faudra peut-être réaliser un réglage fin des paramètres de la stratégie.
Clos (pas d'incident)	Fermé	La stratégie a été violée, mais l'envoi de données protégée a été sanctionné par une disposition spéciale. Aucune mesure complémentaire n'est requise.
Clos (autre)	Fermé	L'incident a été clos pour d'autres raisons

Priorité de l'incident

La priorité de l'incident désigne l'urgence selon laquelle il faut traiter l'incident. L'application attribue une priorité à un incident dès qu'il a été créé (*Faible*, *Moyenne* ou *Elevée*). La priorité est attribuée sur la base de la valeur définie dans les paramètres de la stratégie violée.

Archives des incidents

Les incidents fermés peuvent être déplacés vers une archive (cf. section « Archivage des incidents » à la page 39). Les incidents déplacés vers une archive sont des incidents *archivés*. Les incidents archivés sont supprimés dans la liste des incidents. Si nécessaire, vous pouvez restaurer des incidents depuis l'archive (cf. section « Restauration des incidents depuis l'archive » à la page 39) et les consulter à nouveau dans la liste des incidents.

L'archive des incidents est un fichier dans un format spécial qui porte l'extension bak. Vous pouvez créer un nombre illimité d'archives d'incidents.

Le recours aux archives permet de supprimer à intervalles réguliers les incidents clos de la liste et d'utiliser ainsi de manière optimale le volume de la base de données des incidents sans perdre l'historique des incidents et de leur traitement.

Statistiques et rapports

L'application affiche les statistiques sur les incidents survenus, les incidents en cours de traitement et les incidents fermés. Ces informations permettent d'évaluer l'efficacité du travail de l'expert en sécurité de l'information. Ces données permettent également de créer des rapports.

COLLABORATION ENTRE LES EXPERTS EN SECURITE DE L'INFORMATION

L'application permet la collaboration de plusieurs experts en sécurité de l'information.

Tous les utilisateurs disposant du rôle d'« Expert en sécurité de l'information » dans l'application peuvent accéder à tous les éléments de l'administration et à toutes les fonctions du Module DLP. Les modifications apportées par un expert en sécurité de l'information aux catégories, aux stratégies, aux incidents et aux rapports de l'application sont disponibles pour tous les utilisateurs.

PROCESSUS D'ANALYSE DES MESSAGES PAR LE MODULE DLP

Le module DLP analyse les messages selon l'algorithme suivant :

1. Le module DLP reçoit le message.
2. Le Module DLP vérifie si le message entre ou non dans la zone d'action de chacune des stratégies existantes (cf. section « Création d'une stratégie » à la page 24).
   - Si le message n'appartient à la zone d'action d'aucune des stratégies, le module DLP ignore le message sans aucune modification.
   - Si le message entre dans la zone d'action d'une quelconque stratégie, le Module DLP recherche dans le message des fragments de données correspondant à la catégorie de cette stratégie (cf. section « Présentation des catégories DLP » à la page 8). La recherche porte sur l'objet du message, le corps du texte et toutes les pièces jointes.
3. En cas de résultat positif (le message contenait des équivalences avec une catégories de la stratégie), cela signifie que la stratégie a été violée. Le Module DLP attribue à l'incident créé la priorité indiquée et effectue sur le message les actions indiquées dans les paramètres de la stratégie (cf. section « Modification des paramètres d'une stratégie » à la page 29) :
   - Il supprime le message ou le remet à son destinataire. Une copie du message peut être jointe à l'incident en vue d'une enquête ultérieure.
   - Il envoie une notification sur la violation de la stratégie aux destinataires indiqués (cf. section « Configuration de l'envoi des notifications sur la violation d'une stratégie » à la page 29).

   Les informations sur l'action effectuée sur le message sont conservées dans les informations sur l'incident (cf. section « Consultation des détails relatifs à l'incident » à la page 34).
4. En cas de résultat négatif, le module DLP passe à l'analyse du message selon la stratégie suivante.

Si le message viole la sécurité des informations de plusieurs stratégies simultanément, le module DLP crée plusieurs incidents conformément au nombre de stratégies violées.

Les messages subissent ce traitement sur tous les serveurs de messagerie de votre entreprise dotés du module DLP. Les incidents observés sur tous les serveurs de messagerie de l'entreprise sont repris dans une liste d'incidents uniques. Si, en fonction de la topologie de votre infrastructure de messagerie, un message transite par deux serveurs de messagerie dotés du module DLP ou plus, le message sera soumis à la recherche d'éventuelles fuites sur un seul serveur uniquement. Cela permet d'exclure toute possibilité de duplication des incidents et de perturbation des statistiques dans les rapports (cf. section « Utilisation des rapports » à la page 41).

PRESENTATION DE L'AJOUT D'EN-TETE X

Le module DLP ajoute de nouveaux en-tête X aux messages lors du traitement. Ces en-têtes X permettent, lors de l'analyse du message, d'obtenir des informations sur les résultats de son traitement par le module DLP.

Таблица 3. En-tête X des messages ajoutés par le module DLP

EN-TÊTE X	VALEURS
X-KSE-Dlp-Interceptor-Info	*license violation* : violation de la licence, message remis sans analyse. *protection disabled* : module DLP désactivé ; message remis sans analyse. *fallback* : module DLP inopérationnel ; message remis sans analyse.
X-KSE-DLP-ScanInfo	*Overloaded* file d'attente des messages entrants pleine ; message remis sans analyse. *Skipped* : stratégies applicables au message introuvables ; message remis sans analyse. *Clean* : le message était couvert par la zone d'action d'une ou de plusieurs stratégies, mais aucune violation de stratégie n'a été détectée. *Detect* : le message a entraîné la violation d'une ou de plusieurs stratégies. *ScanError* : erreur d'analyse.

INTERFACE DE L'APPLICATION

La console d'administration assure l'interface d'administration de l'application. Il s'agit d'un composant enfichable isolé spécial intégré à Microsoft Management Console (MMC).

DANS CETTE SECTION

FENETRE PRINCIPALE DE LA CONSOLE D'ADMINISTRATION

La fenêtre principale de la Console d'administration contient les éléments suivants :

- **Menu**. Il se trouve dans la partie supérieure de la fenêtre principale. Le menu permet d'administrer les fichiers et les fenêtres et offre également l'accès aux fichiers d'aide.
- **Arborescence de la Console d'administration**. Se trouve dans la partie gauche de la fenêtre principale. L'arborescence de la Console de gestion permet d'accéder aux fonctions et aux paramètres de l'application.
- **Espace de travail**. Se trouve dans la partie droite de la fenêtre principale. L'espace de travail affiche le contenu de l'entrée sélectionnée dans l'arborescence de la console de gestion.

ARBORESCENCE DE LA CONSOLE D'ADMINISTRATION

L'arborescence de la console contient l'entrée racine **Protection contre les fuites de données** qui reçoit les informations sur l'état de la protection des données contre les fuites.

L'entrée racine contient des sous-entrées prévues pour l'administration des fonctions de l'application :

- **Catégories et stratégies** Configuration des paramètres de protection des données contre les fuites
- **Incidents** Traitement des incidents
- **Rapports**. Création et consultation de rapports sur le fonctionnement du module DLP et autres actions sur ces rapports.

ESPACE DE TRAVAIL

L'espace de travail permet d'accéder au contenu de l'entrée sélectionnée dans l'arborescence de la Console de gestion : aux paramètres, aux fonctions de l'application ou aux informations statistiques relatives au fonctionnement de l'application. Le type d'espace de travail varie en fonction de l'entrée sélectionnée.

LANCEMENT ET ARRET DE L'APPLICATION

Pour commencer à utiliser l'application, vous devez lancer la console d'administration.

Pour lancer la console d'administration,

sélectionnez dans le menu **Démarrer** l'option **Tous les programmes □□Kaspersky Security 9.0 for Microsoft Exchange Servers □□Kaspersky Security 9.0 for Microsoft Exchange Servers**.

Après son lancement, la console d'administration se connecte automatiquement au serveur de sécurité.

Dans l'arborescence de la console d'administration, sélectionnez l'entrée **Protection contre les fuites de données**, puis les entrées suivantes :

- **Catégories et stratégies**
- **Incidents**
- **Rapports**.

Si la console d'administration n'est pas installée sur votre ordinateur ou que vous constatez une différence entre le lancement de la console d'administration et la description faite ici, contactez votre administrateur.

Pour mettre fin à l'utilisation de l'application, vous devez fermer la console d'administration.

Pour fermer la console d'administration,

dans le menu principal de la Console d'administration, sélectionnez l'option **Fichier □□Quitter**.

ÉTAT DE LA PROTECTION DES DONNEES CONTRE LES FUITES

Cette section contient des informations sur l'état par défaut de la protection des données contre les fuites ainsi que des instructions pour obtenir des informations sur l'état du Module DLP et des statistiques concernant le fonctionnement de ce module.

DANS CETTE SECTION

ÉTAT PAR DEFAUT DE LA PROTECTION DES DONNEES CONTRE LES FUITES

Après l'installation de l'application, la protection des données contre les fuites se trouve par défaut dans l'état suivant :

- Le module DLP est activé.
- L'application contient des catégories prédéfinies. L'application ne contient aucune catégorie définie par l'utilisateur.
- L'application ne possède aucune stratégie.
- L'application ne recherche pas les éventuelles fuites de données dans les messages sortant et ne crée pas d'incidents. Le module DLP ignore tous les messages sortant.

CONSULTATION DES INFORMATIONS RELATIVES A L'ETAT DE LA PROTECTION DES DONNEES CONTRE LES FUITES

Les informations sur l'état de la protection contre les fuites de données apparaissent dans la zone de travail de l'entrée **Protection contre les fuites de données** de la Console d'administration.

Les informations reprises dans l'espace de travail de l'entrée **Protection contre les fuites de données** sont réparties en trois groupes :

- **Etat du Module DLP**
- **Incidents ouverts**.
- **statistiques**.

Groupe Etat du Module DLP

Le groupe **Etat du Module DLP** permet d'obtenir des informations sur l'état actuel du module DLP et sur les erreurs survenues pendant le fonctionnement du module DLP sur les serveurs de sécurité de votre organisation. Le groupe contient les informations suivantes :

- Etat du module DLP (*Activé, Activé et fonctionne avec des erreurs, Désactivé*).
- informations sur les types d'erreurs suivant (le cas échéant) :
  - erreurs liées à la licence ;
  - erreurs liées à la base de données DLP ;
  - erreurs d'analyse des messages ;
  - erreurs de communication avec les serveurs de sécurité dotés du module DLP.

  Les groupes contenant les informations relatives aux erreurs reprennent le nombre et la liste de serveurs de sécurité sur lesquels les erreurs se sont produites.

Groupe Incidents ouverts

Le groupe **Incidents ouverts** permet de consulter les statistiques sur les incidents existants portant l'état *Nouveau* et *En cours de traitement*.

La partie supérieure du groupe reprend les informations suivantes :

- **Violateurs**. Nombre d'expéditeurs uniques. Les incidents créés lors de l'analyse des messages de ces expéditeurs possèdent l'état *Nouveau* ou *En traitement*.
- **Nouveaux incidents**. Nombres d'incidents possédant actuellement l'état *Nouveau*.
- **Incidents lors du traitement**. Nombres d'incidents possédant actuellement l'état *En cours de traitement*.
- **Incidents ouverts avec priorité élevée**. Nombre d'incidents ouverts (en pour cent) qui ont possèdent la priorité supérieure *Elevée*. Ce paramètre affiche le niveau de danger actuel. Ce niveau peut avoir une des valeurs suivantes :
  - 0 à 25 %. Faible. Mis en évidence en vert.
  - 25 à 50 %. Moyenne. Mis en évidence en jaune.
  - 50 à 75 %. Elevée. Mis en évidence en rouge.
  - 75 à 100 %. Critique. Mis en évidence en noir.
- **Top 3 des violateurs**. Liste de trois expéditeurs. Les messages de ces expéditeurs ont violé le plus de stratégies et les incidents créés par ces messages possèdent l'état *Nouveau* ou *En cours de traitement*.

La partie inférieure du groupe reprend le diagramme des incidents ouverts qui signalent le nombre d'incidents portant l'état *Nouveau* et *En cours de traitement* comptabilisés pour chaque catégorie. Par défaut, le diagramme est créé su la base des données de toutes les catégories. Vous pouvez modifier la liste des catégories reprises dans la production du diagramme des incidents ouverts.

Pour modifier la liste des catégories reprises dans la production du diagramme des incidents ouverts :

1. Cliquez sur le bouton **Sélectionner les catégories**.

   La fenêtre **Liste des catégories** s'ouvre.

2. Cochez la case en regard des catégories à utiliser pour la génération du diagramme. Cliquez ensuite sur **OK**.

Le contenu du diagramme sera actualisé conformément aux catégories sélectionnées.

Groupe Statistiques

Le groupe **Statistiques** permet d'obtenir des informations sur les messages traités et analysés ainsi que sur les incidents fermés au cours de la période du rapport. La période du rapport peut être égale à 7 ou 30 jours. Vous pouvez sélectionner la période du rapport.

Pour choisir la période du rapport,

cliquez sur le lien **7 jours** ou **30 jours**.

Les données du groupe sont actualisées en fonction de la période de rapport sélectionnée.

La partie supérieure du groupe contient les informations suivantes :

- **Messages traités**. Nombre de messages reçus par le module DLP.
- **Messages analysés**. Nombre de messages entrés dans la zone d'action d'une stratégie (cf. section « Présentation des stratégies DLP » à la page 10) et analysés par le module DLP.
- **Incidents créés**. Nombre d'incidents créés.
- **Messages ignorés à cause des délais d'attente**. Nombre de messages qui n'ont pas été analysés en raison d'un dépassement de la durée d'analyse.
- **Messages ignorés à cause d'erreurs**. Nombre de messages qui n'ont pas été analysés en raison d'erreurs, dont des erreurs liées à la licence.

La partie inférieure du groupe contient le diagramme des incidents fermés qui indique le nombre et le pourcentage d'incidents portant les états *Fermé (traité)*, *Fermé (faux positif)*, *Fermé (n'est pas un incident)*, *Fermé (autre)* créés au cours de la période sélectionnée pour le rapport. Les incidents restaurés depuis l'archive entrent dans la composition du diagramme (cf. section « Restauration des incidents depuis l'archive » à la page 39).

Par défaut, le diagramme est créé su la base des incidents liés à toutes les catégories. Vous pouvez modifier la liste des catégories reprises dans la production du diagramme des incidents fermés.

Pour modifier la liste des catégories reprises dans la production du diagramme des incidents fermés :

1. Cliquez sur le bouton **Sélectionner les catégories**.

   La fenêtre **Liste des catégories** s'ouvre.

2. Cochez la case en regard des catégories à utiliser pour la génération du diagramme. Cliquez ensuite sur **OK**.

Le contenu du diagramme sera actualisé conformément aux catégories sélectionnées.

CONFIGURATION DES ADRESSES DES EXPERTS EN SECURITE DE L'INFORMATION

Lors de l'utilisation du module DLP, il est recommandé de configurer les adresses électroniques des experts en sécurité de l'information. L'application peut envoyer à ces adresses des notifications concernant l'état du module DLP et la violation de stratégies ainsi que des rapports. Cela permet de recevoir des informations opérationnelles sur l'état de la sécurité des informations de l'entreprise.

Pour configurer les adresses des experts en sécurité de l'information, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Protection contre les fuites de données**.

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

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

3. Dans le champ **Adresses des experts en sécurité de l'information** saisissez les adresses en les séparant par un point-virgule.

4. Cliquez sur **OK** pour enregistrer les modifications.

Il est recommandé d'effectuer cette opération à chaque changement de la composition de l'équipe des experts en sécurité de l'information de votre entreprise.

UTILISATION DES CATEGORIES

Cette section contient des instructions pour la création, la modification et la suppression des catégories DLP.

DANS CETTE SECTION

CREATION ET MODIFICATION D'UNE CATEGORIE DE DONNEES TABULAIRES

Pour créer ou modifier la catégorie de données tabulaires, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.
2. Réalisez une des actions suivantes :
   - Si vous souhaitez créer une catégorie de données tabulaires, cliquez sur le bouton **Ajouter une catégorie**. Sélectionnez ensuite l'option **Données tabulaires** dans le menu déroulant.
   - Si vous souhaitez modifier une catégorie de données tabulaires existante, sélectionnez-la dans la liste des catégories et des stratégies, puis cliquez sur le bouton **Modifier**.

   Une fenêtre affichant les paramètres de la catégorie s'ouvre.
3. Indiquez le nom de la catégorie dans le champ **Nom** du formulaire.
4. Cliquez sur le bouton **Parcourir** puis sélectionnez le fichier au format CSV qui contient les informations à protéger contre les fuites à l'aide de la catégorie.

   Le fichier CSV doit être enregistré en UTF-8. Aucun autre type de codage n'est pris en charge.

   La première ligne du fichier CSV est le titre. Cette ligne n'est pas ajoutée et ne participe pas à la création de la catégorie.
5. Dans la liste déroulante **Séparateur de colonnes**, sélectionnez le caractère utilisé dans le fichier pour séparer les colonnes.
6. Dans le groupe **Niveau de correspondance**, indiquez les valeurs seuil des lignes et des colonnes (cf. section « Exemple d'une catégorie de données tabulaires » à la page 21).

   Pour en savoir plus sur les valeurs seuil pour les lignes et les colonnes, cliquez sur le lien **Aide à la configuration du niveau de correspondance** dans la fenêtre **Paramètres de la catégorie.**
7. Saisissez des informations complémentaires en rapport avec les données de la catégorie dans le champ **Commentaires**.
8. Cliquez sur **OK**.

Les informations du fichier seront ajoutées à la catégorie. La catégorie de données tabulaire qui vient d'être créée/modifiée s'affichera dans la liste des catégories et des stratégies.

EXEMPLE D'UNE CATEGORIE DE DONNEES TABULAIRES

Supposons qu'un fichier staff.csv contenant les informations suivantes soit utilisé en tant que données d'origine pour la catégorie de données tabulaires (cf. tableau ci-dessous) :

Таблица 4. Contenu du fichier csv

NOM	NOM	FONCTION	CODE POSTAL	VILLE
Ivan	Petrov	manager	125195	Moscow
John	Smith	developer	SW3	London
Otto	Weber	tester	12277	Berlin

Les valeurs de paramètres suivantes sont utilisées pour la création d'une catégorie :

- **Valeur seuil des colonnes** = 3.
- **Valeur seuil des lignes** = 2.

La stratégie créée sur la base de cette catégorie sera violée si le texte du message analysé contient des valeurs d'au moins trois colonnes (valeur du paramètre **Valeur seuil des colonnes**) d'une ligne et d'au moins deux lignes (valeur du paramètre **Valeur seuil des lignes**). Par ailleurs, plusieurs colonnes peuvent être identifiées sur chaque ligne.

La stratégie créée sur la base de cette catégorie sera violée si le texte du message analysé contient les fragments suivants :

- « manager Ivan Petrov and developer John Smith ».
- « 125195 Moscow Ivan tester Weber Berlin ».

La stratégie créée sur la base de cette catégorie ne sera pas violée si le texte du message analysé contient les fragments suivants :

- « Ivan Petrov manager 125195 Moscow » : ce texte ne contient les informations que d'une seule ligne du tableau.
- « Ivan John tester Otto manager developer » : ce texte ne contient les informations que de deux colonnes du tableau.

CREATION ET MODIFICATION DE MOTS CLES

Pour créer ou modifier la catégorie par mot-clé, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.
2. Réalisez une des actions suivantes :
   - Si vous souhaitez créer une nouvelle catégorie de mot-clé, cliquez sur le bouton **Nouvelle catégorie**. Sélectionnez ensuite l'option **Des mots-clés** dans la liste déroulante.
   - Si vous souhaitez modifier une catégorie de mot-clé existante, sélectionnez-la dans la liste des catégories et stratégies, puis cliquez sur le bouton **Modifier**.

     La fenêtre **Paramètres de la catégorie** s'ouvre. Dans cette fenêtre, vous pouvez ajouter des mots-clés à la catégorie et renommer celle-ci.
3. Définissez les valeurs pour les paramètres suivants :
   - **Nom**.

     Nom attribué à la catégorie.

- **Champ de saisie des mots-clés**.

  Champ de saisie d'un terme ou d'une expression clé utilisé dans la recherche d'un élément de texte concret dans les messages.

  Un *mot clé* désigne le mot ou l'expression que l'application va identifier comme données confidentielles à protéger contre les fuites. Les mots clés apparaissent entre guillemets.

  Par défaut, la recherche sur la base de mots clés ne fait pas la différence entre les majuscules et les minuscules. Si vous souhaitez faire la distinction entre majuscules et minuscules, saisissez « ! » devant le mot clé.

  Exemple :

  « !Kaspersky Lab »

  Cette recherche renverra tout texte où l'expression « Kaspersky Lab » apparaît avec la première lettre de chacun des éléments en majuscule, et les autres lettres en minuscules. Tout texte où l'utilisation des majuscules dans l'expression diffère de l'exemple, comme « kaspersky lab », « kaspersky Lab » ou « KASPERSKY LAB » sera ignoré.

  Une *expression clé* désigne un groupe de un ou plusieurs mots clés unis par les opérateurs AND, OR, NEAR, ONEAR.

  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 »

  Renvoie le texte dans lequel apparaissent les mots « antivirus » et « sécurité ». Le texte contenant un seul de ces mots sera ignoré.

  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 »

  Cette recherche renvoie tout texte contenant « sécurité » ou « protection de l'ordinateur », ou les deux.

  Le caractère de retour à la ligne dans l'expression équivaut également à l'opérateur OR. Un mot clé écrit sur une nouvelle ligne est associé au terme précédent à l'aide de l'opérateur OR qui, dans ce cas, n'est pas affiché.

  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 »

  La recherche renverra tout texte contenant les mots « sécurité » et « système » séparés par six mots au maximum. Les mots peuvent être séparés par des espaces, des caractères de retour à la ligne, des tabulations et d'autres caractères reconnus dans les spécifications Unicode comme caractères d'espace ou de ponctuation.

  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 »

La recherche renverra tout texte où le mot « confidentialité » suit le mot « protection » à quatre mots d'écart maximum. Les mots peuvent être séparés par des espaces, des caractères de retour à la ligne, des tabulations et d'autres caractères reconnus dans les spécifications Unicode comme caractères d'espace ou de ponctuation.

Vous pouvez composer des expressions complexes composées de plusieurs opérateurs. Pour indiquer la priorité des opérateurs dans l'expression, utilisez des parenthèses.

Exemple :

((« technologies » OR « sécurité ») ONEAR(0) « !Kaspersky ») AND « 2014 »

La recherche renverra tout texte contenant le chiffre 2014 et le mot « Kaspersky » directement à la suite du mot « technologies » ou du mot « sécurité ».

Les expressions du type « mot1 » NEAR(n) (« mot2 » AND « mot3 ») et « mot1 » NEAR(n) (« mot2 » NEAR(m) « mot3 ») ne sont pas prises en charge. Le résultat du traitement de ces expressions est inconnu car l'ordre d'exécution des parenthèses est inconnu. La longueur totale des expressions avec des mots clés dans toutes les catégories selon des mots clés ne peut être supérieure à 480 000 caractères.

- **Commentaires**.

  Informations complémentaires en lien avec les données de la catégorie.

4. Cliquez sur **OK** pour enregistrer les modifications apportées.

La catégorie des mots-clés qui vient d'être créée ou modifiée s'affichera dans la liste des catégories et stratégies.

SUPPRESSION D'UNE CATEGORIE

Vous ne pouvez supprimer que les catégories définies par l'utilisateur. Il est impossible de supprimer les catégories de Kaspersky Lab.

Pour supprimer une catégorie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.
2. Dans la liste des catégories et stratégies, sélectionnez la catégorie que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**. Confirmez la suppression dans la boîte de dialogue qui s'ouvre.

La catégorie sélectionnée sera supprimée. Les stratégies associées à cette catégorie seront aussi supprimées. Les incidents créés conformément à ces stratégies seront conservés (cf. section « Consultation de la liste des incidents » à la page 32).

UTILISATION DES STRATEGIES

Cette section contient des instructions sur la création, la modification et la suppression des stratégies DLP.

DANS CETTE SECTION

CREATION D'UNE STRATEGIE

Une stratégie peut être créée à partir d'une catégorie existante. Une même catégorie peut être utilisée pour la création d'un nombre illimité de stratégies (cf. section « Présentation des stratégies DLP » à la page 10).

Pour créer une stratégie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.
2. Dans la liste des catégories et stratégies, sélectionnez la catégorie dans laquelle vous souhaitez créer une stratégie.
3. Cliquez sur le bouton **Nouvelle stratégie**.

   L'assistant de création de stratégie se lance.
4. Suivez les instructions de l'assistant. Pour passer d'une fenêtre à l'autre de l'assistant, utilisez les boutons **Précédent** et **Suivant**.

DANS CETTE SECTION DE L'AIDE

ÉTAPE 1. CONFIGURATION DES PARAMETRES GENERAUX

Configurez les paramètres généraux de la stratégie à cette étape :

- **Nom de la stratégie**.

  Nom attribué à la stratégie. La valeur par défaut est *<Nom de la catégorie> Nouvelle stratégie*. Vous pouvez modifier cette valeur.

  Le nom des stratégies créées sur la base d'une catégorie doivent être uniques. Les stratégies créées sur la base de différentes catégories peuvent porter le même nom.

- **Activer la stratégie directement après la création**.

  Intervention de la stratégie dans la protection des données contre les fuites conformément à ses paramètres.

  Quand la case est cochée, la stratégie devient active après la fin du fonctionnement de l'Assistant. L'application applique la stratégie aux messages et recherche d'éventuelles fuites de données conformément aux paramètres définis dans la stratégie.

  Si la case n'est pas cochée, la stratégie demeure inactive à la fin de l'Assistant et n'intervient pas dans la protection contre les fuites.

  La case est cochée par défaut.

- **Lien vers le document de référence**.

  Lien vers le document reprenant les exigences de sécurité que doit couvrir la stratégie ou un extrait de ce document. Ce champ est facultatif.

Passez à l'étape suivante de l'Assistant.

ÉTAPE 2. CONFIGURATION DE LA ZONE D'ACTION DE LA STRATEGIE : EXPEDITEURS

Cette étape vous permet de définir les expéditeurs qui constituent la zone d'action de la stratégie. L'application appliquera la stratégie aux messages sortants envoyés par ces expéditeurs.

Configurez les paramètres suivants :

- **Tout utilisateur interne**.

  La stratégie s'applique aux messages envoyés par n'importe quel utilisateur de la société.

  Cette option est sélectionnée par défaut.

- **Utilisateurs et groupes sélectionnés**.

  La stratégie s'applique aux messages envoyés par les utilisateurs de la société figurant dans la liste ci-dessous.

  Vous pouvez ajouter ou supprimer des comptes utilisateur et des groupes d'utilisateurs de la liste à l'aide des boutons  et  .

  Vous pouvez ajouter à la liste uniquement des groupes de sécurité d'utilisateurs. Les groupes de distribution ne peuvent pas être ajoutés. Pour obtenir de plus amples informations, contactez l'administrateur.

  Si la liste contient un groupe d'utilisateurs, l'application applique la stratégie aux messages sortants

envoyés par tous les utilisateurs de ce groupe (et de ses sous-groupes).

Par défaut, la liste est vide.

- **Exclusions**.

  Cette liste contient les comptes utilisateur et les groupes de comptes d'utilisateurs de la société dont les messages ne sont pas soumis à la stratégie.

  Vous pouvez ajouter ou supprimer des comptes utilisateur et des groupes d'utilisateurs de la liste à l'aide des boutons  et  .

  Vous pouvez ajouter à la liste uniquement des groupes de sécurité d'utilisateurs. Les groupes de distribution ne peuvent pas être ajoutés. Pour obtenir de plus amples informations, contactez l'administrateur.

  Si une exclusion est définie sous la forme d'un groupe d'utilisateurs, l'application n'applique pas la stratégie aux messages sortants envoyés par les utilisateurs de ce groupe (ou de ses sous-groupes).

  Par défaut, la liste est vide.

Passez à l'étape suivante de l'Assistant.

ÉTAPE 3. CONFIGURATION DE LA ZONE D'ACTION DE LA STRATEGIE : DESTINATAIRES

Cette étape permet de définir les destinataires des messages couverts par la stratégie. L'application appliquera la stratégie aux messages sortants envoyés par ces expéditeurs.

Configurez les paramètres suivants :

- **Tous**.

  La stratégie s'applique aussi bien aux messages adressés aux utilisateurs de la société qu'à ceux adressés aux destinataires externes.

  Cette option est sélectionnée par défaut.

- **Externes uniquement**.

  La stratégie s'applique aux messages adressés à des destinataires externes à la société.

- **Exclusions**.

  La liste contient les comptes utilisateur, les groupes de compte utilisateur ainsi que les adresses de messagerie qui ne seront pas soumis à la stratégie.

  Vous pouvez créer la liste à l'aide des boutons suivants :

  -  : ajouter à la liste l'adresse au format mailbox@domain.com indiquée dans le champ de saisie. Il est possible d'utiliser un masque, tel que *@domain.com.
  -  : ajouter à la liste le compte d'un utilisateur de la société ou un groupe de comptes utilisateur. Vous pouvez ajouter à la liste uniquement des groupes de sécurité d'utilisateurs. Les groupes de distribution ne peuvent pas être ajoutés. Pour obtenir de plus amples informations, contactez l'administrateur.
  -  : supprimer le compte sélectionné de la liste.

  Si une exclusion est définie sous la forme d'un groupe d'utilisateurs, l'application n'applique pas la stratégie aux messages sortants destinés aux utilisateurs de ce groupe (ou de ses sous-groupes).

  Par défaut, la liste est vide.

Passez à l'étape suivante de l'Assistant.

ÉTAPE 4. CONFIGURATION DES ACTIONS

Cette étape vous permet de définir les actions qui seront effectuées par l'application sur les messages ayant violé une stratégie ainsi que de préciser les destinataires à qui l'application enverra des notifications de violation de la stratégie.

Pour définir les actions, configurez les paramètres suivants :

- **Supprimer le message**.

  Suppression des messages qui ont entraîné une violation de la stratégie.

  Si la case est cochée, l'application supprime le message qui a entraîné une violation de la stratégie. Le message est supprimé si la moindre partie de celui-ci (en-tête, contenu ou n'importe quelle pièce jointe) viole la stratégie.

  Si la case est décochée, l'application ignore le message et ne le modifie pas.

  Que la case soit cochée ou non, l'application consigne l'événement en tant que fuite de données potentielles et crée un incident en cas de violation de la stratégie.

  La case est décochée par défaut.

- **Créer des incidents avec priorité**.

  Évaluation du risque lié à une fuite d'informations potentielle.

  La liste déroulante permet de sélectionner la priorité que l'application attribue à l'incident en cas de violation de la stratégie : *Faible*, *Moyenne*, *Elevée*. La priorité désigne le niveau de danger de la violation de la stratégie et l'urgence selon laquelle il faut traiter l'incident.

  La valeur par défaut est de *Faible*.

- **Joindre le message à l'incident**.

  Ajout d'une copie du message aux informations relatives à l'incident.

  Quand la case est cochée, l'application ajoute une copie du message qui a provoqué la violation de la stratégie aux informations relatives à l'incident en vue d'une analyse ultérieure.

  Quand la case est décochée, l'application n'ajoute pas de copie du message aux informations relatives à l'incident.

  La case est cochée par défaut.

- **Consigner l'événement dans le journal des événements Windows®**.

  Ajout d'enregistrements sur les violations de stratégies dans le journal des événements Windows.

  Si la case est cochée, l'application consigne l'événement « Niveau (Level)=Warning; Source (Source)=KSCM8; Code de l'événement (Event ID)=16000 » dans le journal des événements Windows en cas de violation d'une stratégie. La description de l'événement comporte des informations sur l'expéditeur, les destinataires, l'objet du message et la stratégie enfreinte avec ses catégories.

  Les événements de violation de la stratégie sont utiles si vous utilisez des systèmes automatisés de collecte et d'analyse des événements de sécurité (SIEM, Security Information and Event Management) pour le contrôle de l'état de la sécurité informatique de l'entreprise. Grâce à ces événements, vous pouvez obtenir des informations actualisées sur les incidents qui surviennent lorsque vous n'utilisez pas la Console d'administration.

  Si la case est décochée, les événements ne sont pas consignés dans le journal des événements Windows.

  La case est décochée par défaut.

Pour indiquer les destinataires des notifications, configurez les paramètres suivants :

- **A l'expert en sécurité de l'information**.

  Envoi d'une notification sur la violation de la stratégie à l'adresse de l'expert en sécurité de l'information.

  Si la case est cochée, l'application envoie une notification relative à la violation à l'adresse des spécialistes en sécurité des informations. L'adresse ou la liste d'adresses des experts en sécurité de l'information doit être préalablement saisie à l'entrée **Protection des données contre les fuites**.

  Si la case est décochée, l'application n'envoie aucune notification à l'adresse des experts en sécurité de l'information.

  La case est décochée par défaut.

- **Au contrevenant**.

  Envoie d'une notification sur la violation de la stratégie à l'expéditeur du message.

  Si la case est cochée, l'application envoie une notification à l'expéditeur du message qui a violé la stratégie.

  Si la case est décochée, l'application n'envoie aucune notification à l'expéditeur du message.

  La case est décochée par défaut.

- **Au responsable du contrevenant**.

  Envoie d'une notification sur la violation de la stratégie au responsable de l'expéditeur du message.

  Si la case est cochée, l'application envoie une notification au responsable de l'expéditeur du message qui a violé la stratégie. L'application récupère l'adresse du responsable de l'expéditeur dans Active Directory®.

  Si la case est décochée, l'application n'envoie aucune notification au responsable de l'expéditeur du message.

  La case est décochée par défaut.

- **Avancé**.

  Envoie d'une notification sur la violation de la stratégie à des adresses complémentaires.

  Si la case est cochée, l'application envoie une notification relative à la violation à des adresses complémentaires indiquées dans le champ de saisie.

  Si la case n'est pas cochée, l'application n'envoie aucune notification aux adresses complémentaires.

  La case est décochée par défaut.

- **Champ de saisie**.

  Liste des adresses complémentaires des destinataires des notifications. Les adresses de la liste doivent être séparées par un point virgule.

  Le champ est actif si la case **Avancée** a été cochée.

  Le champ est vide par défaut.

Pour quitter l'assistant, cliquez sur **Terminer**.

MODIFICATION DES PARAMETRES D'UNE STRATEGIE

Pour modifier les paramètres de la stratégie, procédez comme suit :

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

   La fenêtre **Paramètres de la stratégie** s'ouvre.
3. Modifiez les paramètres repris dans les ongles de la fenêtre. Les paramètres dans les onglets de la fenêtre sont identiques aux paramètres des fenêtres de l'assistant de création d'une stratégie (cf. section « Création d'une stratégie » à la page 24).
4. Cliquez sur **OK** pour enregistrer les modifications.

CONFIGURATION DE L'ENVOI DES NOTIFICATIONS SUR LA VIOLATION D'UNE STRATEGIE

Pour chaque stratégie, vous pouvez configurer l'envoi des notifications sur la violation de la stratégie Grâce à ces notifications, vous et d'autres personnes concernées (par exemple les administrateurs, les responsables et d'autres experts en sécurité de l'information) pouvez être informés de manière efficace sur les menaces de fuites de données.

Les notifications de violation de stratégies contiennent les informations suivantes :

- Nom de la stratégie violée.
- Nom de la catégorie conformément à laquelle un incident a été créé.
- Informations sur le message : objet, adresse de l'expéditeur et liste d'adresses des destinataires.
- Numéro de l'incident, date et heure de création de l'incident.
- Contexte de la violation, c'est-à-dire extrait du texte du message ou de la pièce jointe dans lequel figure les données protégées.
- Informations concernant la suppression du message si celui-ci a été supprimé en application de la stratégie.

Les notifications de violation des stratégies sont envoyées par courrier électronique au moment où se produit la violation. Par défaut, l'envoi de notifications est activé dans les paramètres des stratégies.

Pour configurer l'envoi de notifications sur les violations des stratégies, procédez comme suit :

1. Sélectionnez l'entrée **Catégories et stratégies**.

   Une liste des catégories et des stratégies apparaît dans l'espace de travail.
2. Dans la liste, sélectionnez les catégories et les stratégies et appuyez sur le bouton **Paramètres**.

   La fenêtre **Paramètres de la stratégie** s'ouvre.
3. Cliquez sur l'onglet **Actions**.

4. Cochez les cases correspondant aux personnes qui doivent recevoir les notifications : **À l'expert en sécurité de l'information**, **À l'expéditeur**, **Au responsable de l'expéditeur**.

   Lorsque vous cochez la case **À l'expert en sécurité de l'information**, les notifications sont envoyées aux adresses définies dans la liste d'adresses des experts en sécurité de l'information. Lorsque vous cochez la case **Au responsable du contrevenant**, les notifications ne sont envoyées que si l'adresse du responsable de l'expéditeur peut être obtenue dans Active Directory®.

5. Si vous souhaitez configurer l'envoi de notifications à d'autres personnes de votre choix, procédez comme suit :

   a. Cochez la case **Avancé**.

      Le champ de saisie sous la case est alors accessible.

   b. Dans le champ, saisissez les adresses électroniques des destinataires séparées par un point-virgule.

6. Cliquez sur **OK** pour enregistrer les modifications.

Les modifications effectuées seront enregistrées dans la stratégie. Si un incident lié à la violation de cette stratégie se produit, l'application enverra des notifications contenant les informations sur la violation aux adresses électroniques spécifiées.

Les notifications sur les violations de stratégies ne sont envoyées avec succès que si les paramètres d'envoi des notifications sont correctement configurés (adresse et informations d'identification du service en ligne). Pour obtenir de plus amples informations, contactez l'administrateur.

SUPPRESSION D'UNE STRATEGIE

Pour supprimer une stratégie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.

2. Dans la liste des catégories et stratégies, sélectionnez la stratégie que vous souhaitez supprimer.

3. Cliquez sur le bouton **Supprimer**. Confirmez la suppression dans la fenêtre qui s'ouvre.

La stratégie sélectionnée sera supprimée. Les incidents créés conformément à cette stratégie seront conservés (cf. section « Consultation de la liste des incidents » à la page 32).

RECHERCHE DE STRATEGIES RELATIVES A DES UTILISATEURS DEFINIS

L'application permet d'établir la liste des stratégies dans la zone d'action desquelles entre un utilisateur défini. Cette liste contient les informations sur les stratégies qui sont appliquées aux messages sortants de cet utilisateur et sur les actions exécutées par l'application sur les messages conformément à ces stratégies. Ces informations peuvent être utiles pour l'analyse et la rationalisation des paramètres de stratégies conformément aux exigences relatives à la sécurité des informations de l'entreprise.

Pour retrouver les stratégies associées à un utilisateur défini, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Catégories et stratégies**.

2. Dans la section **Recherche de stratégies**, appuyez sur le bouton **Sélectionner**, sélectionnez un utilisateur dans Active Directory et appuyez sur **OK**.

Dans le tableau figurant en bas de la section, la liste des stratégies par lesquelles l'utilisateur défini est concerné apparaît. Lorsqu'il reçoit un message de cet utilisateur, le Module DLP lui applique les stratégies affichées si elles sont actives.

Le tableau contient les informations suivantes concernant les stratégies :

- Nom de la stratégie.
- Nom de la catégorie sur la base de laquelle la stratégie a été créée.
- Action sur les messages qui violent cette stratégie :
    - *Supprimer.* L'application supprime les messages qui violent cette stratégie.
    - *Ignorer.* L'application ignore les messages qui violent cette stratégie.
    - *Inactive.* La stratégie n'est pas active. Le logiciel n'applique pas la stratégie aux messages.

Vous pouvez relancer la recherche et mettre à jour le contenu de la liste en appuyant sur le bouton **Mettre à jour**. Il est possible que l'application vous demande de mettre la liste à jour pour tenir compte de modifications apportées aux stratégies par d'autres experts en sécurité de l'information.

TRAITEMENT DES INCIDENTS

Cette section contient des instructions sur le traitement des incidents créés.

DANS CETTE SECTION

CONSULTATION DE LA LISTE DES INCIDENTS

Afin de consulter la liste des incidents,

Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

L'espace de travail de l'entrée affiche le tableau des incidents.

Le tableau contient une liste des incidents pouvant inclure les nouveaux incidents, les incidents en cours de traitement, les incidents traités et les incidents restaurés depuis l'archive. Cette liste ne contient pas les incidents archivés.

Ce tableau contient les colonnes suivantes :

- **N°**. Numéro d'ordre attribué à l'incident lors de sa création.
- **Etat**. Etat de l'incident. L'état de l'incident indique son stade de traitement, par exemple : *Nouveau*, l'incident a eu lieu, mais n'a pas encore été traité ; *Fermé (traité)*, l'analyse de l'incident est terminée, les mesures requises ont été prises.
- **Objet**. Contenu du champ « Objet » du message dont l'analyse a déclenché la création de l'incident.
- **Expéditeur**. Contenu du champ « De » du message dont l'analyse a déclenché la création de l'incident.
- **Destinataires**. Adresses de tous les destinataires repris dans les champs « A », « Cc » et « Cci » dans l'en-tête du message dont l'analyse a déclenché la création de l'incident.
- **Créé le**. Date et heure de création de l'incident. S'affiche selon le format défini dans les

paramètres régionaux de votre ordinateur.

- **Catégorie**. Nom de la catégorie de données conformément à laquelle un incident a été créé.
- **Stratégie**. Nom de la stratégie qui n'a pas été respectée et qui a entraîné la création d'un incident.
- **Priorité**. Priorité attribuée à un incident lors de sa création (*Faible*, *Moyenne* ou *Elevée*). Elle désigne l'urgence selon laquelle l'incident doit être traité. La priorité est attribuée sur la base de la valeur définie dans les paramètres de la stratégie violée.
- **Action**. Action exécutée sur le message (*Ignoré*, *Supprimé*). L'action à exécuter sur le message est définie dans la stratégie.
- **Violations**. Nombre de fragments de texte du message ayant entraîné une violation de la stratégie.
- **Identifiant du message**. Identifiant unique du message. Contenu du champ « Message-ID » de l'en-tête du message.
- **Nom du serveur**. Nom du serveur de messagerie sur lequel a été créé l'incident.
- **Responsable**. Nom du compte utilisateur du responsable de l'expéditeur du message. Si les informations sur le compte utilisateur du responsable ne sont pas accessibles, le champ affichera la valeur « n/a ».

Le tableau affiche par défaut toutes les colonnes sauf les colonnes **Identifiant du message**, **Nom du serveur** et **Responsable**. Vous pouvez modifier la sélection des colonnes du tableau en cliquant sur **Sélectionner les colonnes**. La colonne **N°** est toujours affichée.

Vous pouvez modifier l'ordre des colonnes en faisant glisser leur titre à l'aide de la souris.

Vous pouvez trier le contenu du tableau par ordre croissant ou décroissant en cliquant sur le bouton gauche de la souris sur les titres des colonnes.

SELECTION DES COLONNES A AFFICHER DANS LE TABLEAU DES INCIDENTS

Vous pouvez sélectionner les colonnes à afficher dans le tableau des incidents : ajouter des colonnes contenant des informations importantes pour vous et masquer celles contenant des informations peu importantes.

Pour sélectionner les colonnes à afficher dans le tableau des incidents, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.
2. Dans le groupe **Liste des incidents**, cliquez sur le bouton **Sélectionner les colonnes**.

   Le groupe **Sélection des colonnes à afficher** se développe.
3. Cochez les cases correspondant aux colonnes qui doivent s'afficher dans le tableau. Décochez les cases correspondant aux colonnes qui doivent être masquées dans le tableau.

Les modifications s'appliquent au tableau dès que les cases sont cochées ou décochées. La colonne **№** indiquée par l'icône dans la fenêtre **Sélection des colonnes à afficher** est toujours visible dans le tableau.

FILTRAGE DE LA LISTE DES INCIDENTS

Vous pouvez filtrer la liste des incidents en fonction d'une ou de plusieurs conditions à l'aide d'un filtre d'incidents. Les conditions du filtre s'appliquent aux colonnes du tableau. En ajoutant des conditions, vous pouvez créer des filtres complexes. Vous pouvez combiner les conditions du filtre à l'aide de l'opérateur logique « ET ». Les incidents qui ne correspondent pas aux conditions du filtre ne figurent pas dans la liste.

Par défaut, le filtre « État Ouverts » s'applique à la liste des incidents. La liste contient donc les incidents ouverts dont l'état est *Nouveau* et *En cours de traitement*.

Pour filtrer la liste des incidents, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.
2. Dans la section **Filtre des incidents**, définissez les conditions du filtre :
   a. Dans la liste qui s'ouvre, sélectionnez les colonnes auxquelles la condition doit s'appliquer.

      En fonction de la colonne sélectionnée, les paramètres de la condition peuvent prendre les formes suivantes :

      - liste déroulante ;
      - champ de saisie ;
      - liste déroulante et champ de saisie.

   b. Sélectionnez la valeur du paramètre (ou des paramètres) dans la liste déroulante ou indiquez-la manuellement.
3. Si nécessaire, ajoutez des critères de filtre supplémentaires en appuyant sur le bouton **Ajouter une condition**. Supprimez les conditions inutiles à l'aide du bouton  situé à droite de la ligne contenant la condition.
4. Cliquez sur le bouton **Appliquer le filtre** pour filtrer la liste des incidents.

L'application affiche les incidents correspondant aux conditions du filtre. Les incidents qui ne correspondent pas aux conditions du filtre seront masqués.

CONSULTATION DES DETAILS RELATIFS A L'INCIDENT

Pour consulter les informations détaillées sur l'incident, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.
2. Dans la liste, sélectionnez l'incident souhaité puis cliquez sur le bouton **Consulter**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Détails de l'incident** s'ouvre. Elle contient des informations détaillées sur l'incident sélectionné. Vous pouvez naviguer entre les incidents de la liste à l'aide des boutons **Suivant** et **Précédent**.

   La fenêtre contient les informations suivantes sur l'incident :

   - **N°**. Numéro d'ordre attribué à l'incident lors de sa création.
   - **Objet du message**. Contenu du champ « Objet » du message dont l'analyse a déclenché la création de l'incident.
   - **Destinataires**. Adresses de tous les destinataires repris dans les champs « A », « Cc » et « Cci » dans l'en-tête du message dont l'analyse a déclenché la création de l'incident.
   - **Expéditeur**. Contenu du champ « De » du message dont l'analyse a déclenché la création de l'incident.
   - **Responsable de l'expéditeur**. Nom du compte utilisateur du responsable de l'expéditeur du message. Si les informations sur le compte utilisateur du responsable ne sont pas accessibles, le champ affichera la valeur « n/a ».

- **Stratégie**. Nom de la stratégie qui n'a pas été respectée et qui a entraîné la création d'un incident.
- **Catégorie**. Nom de la catégorie de données conformément à laquelle un incident a été créé.
- **Action**. Action exécutée sur le message (Ignoré, Supprimé). L'action à exécuter sur le message est définie dans la stratégie.
- **Créé le**. Date et heure de création de l'incident. S'affiche selon le format défini dans les paramètres régionaux de votre ordinateur.
- **Priorité**. Priorité attribuée à un incident lors de sa création (*Faible*, *Moyenne* ou *Elevée*). Elle désigne l'urgence selon laquelle l'incident doit être traité. La priorité est attribuée sur la base de la valeur définie dans les paramètres de la stratégie violée.
- **Etat**. Etat de l'incident. L'état de l'incident indique son stade de traitement, par exemple : Nouveau, l'incident a eu lieu, mais n'a pas encore été traité ; Fermé (traité), l'analyse de l'incident est terminée, les mesures requises ont été prises.
- **Violations**. Nombre de fragments de texte du message ayant entraîné une violation de la stratégie.
- **Contexte des violations**. Extraits de texte contenant les données qui ont provoqué la violation de la stratégie. Les mots clés ou les données du tableau sont mises en évidence en rouge dans chaque extrait. Le contexte permet d'accélérer le traitement de l'incident.

MODIFICATION DE L'ETAT DES INCIDENTS

Vous pouvez modifier l'état des incidents d'une des deux méthodes suivantes :

- Dans la liste des incidents. Cette méthode permet de modifier l'état de plusieurs incidents.
- Dans la fenêtre reprenant les détails de l'incident. Cette méthode permet de modifier l'état d'un incident.

Pour modifier l'état des incidents dans la liste des incidents, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Réalisez une des actions suivantes :

   - Si vous souhaitez modifier l'état de tous les incidents, repris dans la liste, cliquez sur le bouton **Modifier l'état** et choisissez l'option **Tous les incidents**.

     L'état des incidents masqués par le filtre n'est pas modifié.

   - Si vous souhaitez modifier l'état de certains incidents, procédez comme suit :

     a. Dans la liste, sélectionnez les incidents dont vous souhaitez modifier l'état. Vous pouvez sélectionner un ou plusieurs incidents.

     b. Cliquez sur le bouton **Modifier l'état**, puis choisissez l'option **Événements sélectionnés**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Modification de l'état** s'ouvre.

3. Dans la liste déroulante **Etat**, sélectionnez l'état que vous souhaitez attribuer aux incidents.

4. La modification de l'état des incidents peut être accompagnée de commentaires. Si vous souhaitez ajouter des commentaires, saisissez le texte dans le champ **Commentaires**.

5. Cliquez sur **OK** pour enregistrer les modifications.

   Si vous avez choisi de modifier l'état de plusieurs ou de l'ensemble des incidents, la fenêtre de confirmation de l'action s'ouvre.

6. Dans la fenêtre ouverte, confirmez la modification de l'état en cliquant sur le bouton **Oui**.

L'état des incidents sélectionnés sera modifié. Un comment peut être ajouté aux incidents sélectionnés si ce commentaire a été saisi.

Les informations relatives à la modification de l'état de chaque incident et au commentaire qui l'accompagne sont conservées dans l'historique de la modification de l'incident. L'historique des modifications d'un incident est disponible dans la fenêtre présentant les détails relatifs à cet incident (cf. section « Consultation des détails relatifs à l'incident » à la page 34).

Pour modifier l'état d'un incident au départ de la fenêtre des détails de l'incident, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Sélectionnez l'incident dont vous souhaitez modifier l'état, puis cliquez sur le bouton **Consulter**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Détails de l'incident** s'ouvre.

3. Dans l'onglet **Parcourir**, appuyez sur le bouton **Modifier** dans le champ **État**.

   La fenêtre **Modification de l'état** s'ouvre.

4. Dans la liste déroulante **État**, sélectionnez l'état que vous souhaitez attribuer à l'incident.

5. La modification de l'état de l'incident peut être accompagnée de commentaires. Si vous souhaitez ajouter des commentaires, saisissez le texte dans le champ **Commentaires**.

6. Cliquez sur **OK** pour enregistrer les modifications.

ENREGISTREMENT SUR LE DISQUE DE MESSAGES LIES A UN INCIDENT

Les messages liés à des incidents peuvent contenir des informations confidentielles. Afin de protéger la confidentialité des données, l'enregistrement sur le disque d'un message lié à un incident est consigné sur le Serveur de sécurité. Pour obtenir de plus amples informations, contactez l'administrateur.

Pour enregistrer sur le disque un message lié à un incident, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Dans la liste, sélectionnez l'incident souhaité puis cliquez sur le bouton **Consulter**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Détails de l'incident** s'ouvre. Elle contient des informations détaillées sur l'incident sélectionné.

3. Cliquez sur le bouton **Actions** situé à droite du champ **Objet du message** et sélectionnez l'option **Enregistrer le message**.

   La boîte de dialogue **Enregistrer sous** s'ouvre.

4. Sélectionnez le dossier de destination où vous voulez enregistrer le message, puis cliquez sur le bouton **Enregistrer**.

Le message sera enregistré dans le dossier de destination au format EML.

L'événement « Niveau (Level)=Warning; Source (Source)=KSCM8; Code de l'événement (Event ID)=16012 » figurera dans le journal des événements Windows sur le Serveur de sécurité. Il contiendra le texte suivant : L'expert en sécurité de l'information a tenté de sauvegarder sur le disque un message lié à un incident.

Pour obtenir de plus amples informations, contactez l'administrateur.

ENVOI D'UNE NOTIFICATION AU CONTREVENANT

Vous pouvez envoyer une notification relative à la violation d'une stratégie à l'adresse du contrevenant (expéditeur du message qui a provoqué l'incident). L'envoi de ce genre de notification peut faire partie de la procédure de traitement des incidents adoptée par votre organisation.

Une copie de la notification est également envoyée au supérieur du contrevenant, à condition que l'adresse de ce supérieur soit disponible dans Active Directory.

Cette action est possible si votre ordinateur est doté d'un client de messagerie configuré comme il se doit.

Pour envoyer une notification au contrevenant, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Dans la liste, sélectionnez l'incident souhaité puis cliquez sur le bouton **Consulter**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Détails de l'incident** s'ouvre. Elle contient des informations détaillées sur l'incident sélectionné. Le champ **Expéditeur** accueille l'adresse du contrevenant qui apparaît sous la forme d'un lien.

3. Cliquez sur le lien dans le champ **Expéditeur**.

   Une fenêtre du client de messagerie par défaut de votre ordinateur s'ouvre. Le texte du nouveau message apparaît dans la fenêtre :

   Bonjour, Le message dont le sujet était "<objet du message>" a été envoyé de votre adresse <adresse du contrevenant> le <date et heure d'envoi du message> aux destinataires suivants : <adresse des destinataires>. Ce message contenait des informations confidentielles, ce qui va à l'encontre de la stratégie de sécurité de l'information adoptée par l'organisation.

4. Le cas échéant, modifiez le texte de la notification. Envoyez ensuite la notification via le client de messagerie.

La notification sera envoyée au contrevenant et à son supérieur, si l'adresse de ce dernier a pu être récupérée dans Active Directory.

Vous pouvez également configurez les paramètres de la stratégie de sorte que les notifications relatives aux violations de la stratégie soient envoyées au contrevenant directement lors de la création de l'incident (cf. section « Etape 4. Configuration des actions » à la page 27).

AJOUT D'UN COMMENTAIRE AUX INCIDENTS

Vous pouvez commenter les incidents. Ceci est utile lorsqu'il est nécessaire de consigner des informations complémentaires relatives à l'incident durant l'enquête.

Deux méthodes existent pour ajouter des commentaires :

- Dans la liste des incidents. Cette méthode permet d'ajouter des commentaires à plusieurs incidents.
- Dans la fenêtre reprenant les détails de l'incident. Cette méthode permet d'ajouter des commentaires à un incident.

Pour ajouter des commentaires aux incidents de la liste, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Si vous souhaitez commenter tous les incidents repris dans la liste, cliquez sur le bouton **Modifier l'état**, puis choisissez l'option **Tous les incidents**.

   Les commentaires ne sont pas ajoutés aux incidents masqués par le filtre.

3. Si vous souhaitez commenter certains incidents, procédez comme suit :

   a. Dans la liste, sélectionnez les incidents que vous souhaitez commenter. Vous pouvez sélectionner un ou plusieurs incidents.

   b. Cliquez sur le bouton **Modifier l'état**, puis choisissez l'option **Événements sélectionnés**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Modification de l'état** s'ouvre.

4. Saisissez le texte du commentaire dans le champ **Commentaires**.

5. Cliquez sur **OK** pour enregistrer les modifications.

6. Si vous avez commenter plusieurs incidents ou l'ensemble de ceux-ci, cliquez sur le bouton **Oui** dans la fenêtre qui s'ouvre.

Le commentaire sera ajouté aux incidents sélectionnés.

Les commentaires de chaque incident sont conservés dans l'historique des modifications de l'incident. L'historique des modifications d'un incident est disponible dans la fenêtre présentant les détails relatifs à cet incident (cf. section « Consultation des détails relatifs à l'incident » à la page 34).

Pour commenter un incident au départ de la fenêtre des détails de l'incident, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.

   Le tableau contenant la liste des incidents apparaît dans l'espace de travail.

2. Sélectionnez l'incident que vous souhaitez commenter, puis cliquez sur le bouton **Consulter**. Vous pouvez également exécuter cette action à l'aide du menu contextuel.

   La fenêtre **Détails de l'incident** s'ouvre.

3. Saisissez le texte du commentaire dans le champ **Commentaires** de l'onglet **Historique**.

4. Cliquez sur **OK** pour enregistrer les modifications.

ARCHIVAGE DES INCIDENTS

Les fichiers archives peuvent contenir des informations confidentielles. Afin de protéger la confidentialité des données archivées, la création d'une archive est consignée sur le Serveur de sécurité. Pour obtenir de plus amples informations, contactez l'administrateur.

Pour archiver des incidents, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.
2. Cliquez sur le bouton **Archiver**.

   L'Assistant d'archivage des incidents s'ouvre. La première fenêtre de l'Assistant reprend les informations relatives au nombre d'incidents qui peuvent être archivés ainsi que le nombre d'incidents qui ne peuvent pas être archivés.

   Seuls les incidents clos, à savoir les incidents portant l'état *Clos (<raison>)* peuvent être placés dans une archive. Si la liste ne contient aucun incident de ce type, l'archivage n'est pas possible.

   Les incidents archivés, puis restaurés dans la liste des incidents ne peuvent pas être archivés à nouveau. Ces incidents sont accompagnés de l'icône *archivé* dans le champ **Etat**. L'Assistant les ignore lors de l'archivage.
3. Si l'Assistant ne trouve aucun incident clos dans la liste, il se peut qu'ils aient été masqués par un filtre Dans ce cas, arrêtez l'Assistant en cliquant sur le bouton **Annuler**. Annulez ensuite le filtre ou modifiez ses conditions, puis relancez l'Assistant de création d'une archive.
4. Cliquez sur le bouton **Parcourir** et dans la fenêtre qui s'ouvre, saisissez le nom et de dossier de destination du fichier de l'archive.
5. Cliquez sur le bouton **Suivant**.

   Le fichier d'archive sera créé sous le nom indiqué dans le dossier désigné. Les incidents clos seront placés dans l'archive. La fenêtre de l'Assistant affiche le nombre d'incidents placés dans l'archive et le nombre d'incidents ignorés.

   L'événement « Niveau (Level)=Warning; Source (Source)=KSCM8; Code de l'événement (Event ID)=16013 » figurera dans le journal des événements Windows sur le Serveur de sécurité. Il contiendra le texte suivant : L'expert en sécurité de l'information a créé une archive d'incidents.

   Pour obtenir de plus amples informations, contactez l'administrateur.
6. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

Les incidents placés dans l'archive seront supprimés de la liste des incidents.

L'application ne tient pas compte des incidents archivés lors de la création de rapports et de l'envoi d'informations statistiques.

RESTAURATION DES INCIDENTS DEPUIS L'ARCHIVE

Pour restaurer des incidents depuis une archive, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud **Incidents**.
2. Cliquez sur le bouton **Restaurer**.

   L'Assistant de restauration démarre.

3. Sélectionnez les incidents que vous souhaitez restaurer :

   - Si vous souhaitez restaurer tous les incidents de l'archive, choisissez l'option **Tous les incidents**.

   - Si vous souhaitez restaurer uniquement les incidents créés au cours d'une période définie, choisissez l'option **Pour la période**. Saisissez ou sélectionnez en bas les dates de début et de fin de la période. Par défaut, les champs désignent une période qui équivaut au jour d'aujourd'hui.

4. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier d'archive dans la fenêtre qui s'ouvre.

5. Cliquez sur le bouton **Suivant**.

   La fenêtre de l'Assistant affiche le nombre d'incidents restaurés et le nombre d'incidents ignorés.

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

Les incidents restaurés depuis l'archive apparaissent dans la liste des incidents avec l'icône *archive* dans le champ **État**.

L'application tient compte des incidents restaurés des archives lors de la création de rapports et dans les statistiques.

Vous pouvez consulter les informations détaillées sur les incidents restaurés des archives et réaliser d'autres opérations sur ceux-ci, à l'exception de la modification de l'état, de l'ajout de commentaires et de l'archivage de ces incidents. Vous pouvez également supprimer les incidents restaurés de la liste des incidents (cf. section « Suppression des incidents archivés » à la page 40).

SUPPRESSION DES INCIDENTS ARCHIVES

Vous pouvez également supprimer les incidents archivés de la liste des incidents.

Pour supprimer des incidents archivés, procédez comme suit :

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

2. Cliquez sur le bouton **Supprimer les archivés** situé sous la liste des incidents.

3. Confirmez la suppression dans la fenêtre qui s'ouvre.

L'application supprime les incidents accompagnés de l'icône *d'archive* de la liste des incidents.

UTILISATION DES RAPPORTS

Cette section contient des informations relatives aux rapports sur le fonctionnement du module DLP, des instructions sur la création, la consultation, l'enregistrement et la suppression de rapports ainsi que sur la création, la modification, l'exécution et la suppression des tâches de création de rapports.

DANS CETTE SECTION

PRESENTATION DES RAPPORTS SUR LE FONCTIONNEMENT DU MODULE DLP

L'application permet de créer et de consulter des rapports sur le fonctionnement du Module DLP.

L'application permet de créer les types de rapport suivant :

- Rapport détaillé (à la page 42) ;
- Rapport par utilisateur (cf. page 43) ;
- Rapport ICP (KPI) du système (cf. page 44) ;
- Rapport par stratégie et par incident (à la page 45).

Les rapports peuvent être créés d'une des manières suivantes :

- Créer les rapports manuellement (cf. section « Création manuelle d'un rapport » à la page 54).

  Lors de la création manuelle d'un rapport, il faut désigner la période couverte. Par défaut, le rapport est créé pour la journée en cours.

- Créer les rapports à l'aide de tâches de composition de rapports (cf. section « Création d'une tâche de composition d'un rapport » à la page 45).

  Les tâches de composition de rapports peuvent être lancées manuellement (cf. section « Lancement d'une tâche de composition d'un rapport » à la page 53) ou automatiquement selon une planification établie. La première exécution de la tâche a lieu à l'heure définie dans la planification. Les exécutions suivantes ont lieu à intervalles réguliers conformément à la planification. Les exécutions qui ont échoué ainsi que les tâches lancées manuellement n'ont aucune influence sur la planification des tâches.

  La période couverte par le rapport correspond aux intervalles de lancement :

  - **Tous les N jours**. période de N jours ;
  - **Chaque semaine**. période de 7 jours ;
  - **Chaque mois**. période égale au nombre de jours compris entre le jour actuel et le jour équivalent du mois précédent. Si le jour actuel est supérieur au nombre de jours du mois précédent, la date initiale sera le dernier jour du mois précédent.

  L'heure de début et de fin d'une période est 00h00.

  Vous pouvez créer de nouvelles tâches de composition de rapports, supprimer des tâches existantes ou modifier les paramètres des tâches déjà créées.

Les rapports créés manuellement ou à l'aide de tâches de créations de rapports sont conservés dans la liste des rapports. Vous pouvez consulter les rapports créés (cf. section « Consultation d'un rapport » à la page 53), les enregistrer sur le disque (cf. section « Enregistrement des rapports sur le disque » à la page 54) ou les recevoir par courrier électronique. Les rapports envoyés par courrier électronique sont présentés dans un fichier en pièce jointe.

RAPPORT DETAILLE

Un rapport détaillé peut contenir des informations confidentielles dans le champ « Objet ». Avec les rapports de ce type, il est nécessaire de respecter la politique de confidentialité définie par l'entreprise.

Le rapport détaillé contient la liste détaillée des incidents qui se sont produits au cours d'une période donnée. Le rapport reflète l'activité des utilisateurs en lien avec les informations confidentielles.

L'en-tête du rapport contient les informations suivantes :

- **Nom du rapport**. « Rapport détaillé par incident ».
- **<Date>**. Date de création du rapport.
- **<Heure>**. Heure de création du rapport.
- **Nombre d'incidents**. Nombre d'incidents dont les informations sont reprises dans le rapport.
- **Pour la période**. Période pour laquelle le rapport est créé.
- **Par état**. Liste des états des incidents inclus dans le rapport.

- **Par utilisateur et par groupe**. Liste des comptes utilisateur et/ou des groupes. Le rapport contient les incidents crées lors de l'analyse des messages envoyés par les utilisateurs listés. Si un groupe figure dans la liste, le rapport contient les incidents provoques par tous les utilisateurs appartenant à ce groupe et a ses sous-groupes.

- **Par catégorie et par stratégie** Liste des catégories et des stratégies. Le rapport contient des incidents en lien avec ces catégories et ces stratégies. Si la mention « Toutes les catégories et stratégies » figure dans le champ, le rapport contient également les incidents en lien avec les catégories et stratégies supprimées.

Plus bas, un tableau reprend tous les incidents groupés par stratégie violée. Chaque stratégie correspond à un tableau dans le rapport. Les tableaux contiennent les informations suivantes concernant les incidents :

- **N°**. Numéro d'ordre attribué à l'incident lors de sa création.

- **Etat**. Etat de l'incident. L'état de l'incident indique son stade de traitement, par exemple : *Nouveau*, l'incident a eu lieu, mais n'a pas encore été traité ; *Fermé (traité)*, l'analyse de l'incident est terminée, les mesures requises ont été prises.

- **Violations**. Nombre de fragments de texte du message ayant entraîné une violation de la stratégie.

- **Expéditeur**. Contenu du champ « De » du message dont l'analyse a déclenché la création de l'incident.

- **Responsable**. Nom du compte utilisateur du responsable de l'expéditeur du message. Si les informations sur le compte utilisateur du responsable ne sont pas accessibles, le champ affichera la valeur « n/a ».

- **Créé le**. Date et heure de création de l'incident. S'affiche selon le format défini dans les paramètres régionaux de votre ordinateur.

- **Destinataires**. Adresses de tous les destinataires repris dans les champs « A », « Cc » et « Cci » dans l'en-tête du message dont l'analyse a déclenché la création de l'incident.

- **Objet**. Contenu du champ « Objet » du message dont l'analyse a déclenché la création de l'incident.

- **Identifiant du message**. Identifiant unique du message. Contenu du champ « Message-ID » de l'en-tête du message.

- **Action**. Action exécutée sur le message (*Ignoré*, *Supprimé*). L'action exécutée sur le message est définie dans les paramètres de violation de la stratégie.

Les lignes dans les tableaux sont triées en fonction de la valeur du paramètre **Trier les données par colonne**, indiquée dans les paramètres du rapport ou de la tâche de composition de rapports (cf. section « Tâche de composition d'un rapport détaillé : configuration des paramètres » à la page 46).

Le rapport peut contenir les informations sur un maximum de 50000 incidents.

RAPPORT PAR UTILISATEUR

Le rapport par utilisateur contient les informations sur le nombre d'incidents créés conformément à des catégories définies. Les incidents sont regroupés dans le rapport par utilisateurs qui ont envoyé des messages contenant des données protégées au cours de la période définie. Le rapport indique le nombre de violations de stratégies pour chaque catégorie provoquées par chacun de ces utilisateurs.

L'en-tête du rapport contient les informations suivantes :

- **Nom du rapport**. « Par utilisateur ».

- **<Date>**. Date de création du rapport.

- **<Heure>**. Heure de création du rapport.

- **Nombre d'incidents**. Nombre d'incidents dont les informations sont reprises dans le rapport.

- **Pour la période**. Période pour laquelle le rapport est créé.
- **Par état**. Liste des états des incidents inclus dans le rapport.
- **Par utilisateur et par groupe**. Liste des comptes utilisateur et/ou des groupes. Le rapport contient les incidents crées lors de l'analyse des messages envoyés par les utilisateurs listés. Si un groupe figure dans la liste, le rapport contient les incidents provoques par tous les utilisateurs appartenant à ce groupe et a ses sous-groupes.
- **Catégories**. Liste des catégories. Le rapport reprend les incidents créés conformément à ces catégories. Si le champ contient la valeur « Toutes les catégories », le rapport reprend également les incidents créés conformément aux catégories supprimées.

En bas se trouve un tableau reprenant la liste des utilisateurs repris dans le rapport. Les tableaux affichent les informations suivantes sur les utilisateurs :

- **Utilisateur**. Nom du compte utilisateur et adresse de messagerie.
- **Section**. Service, département ou autre division organisationnelle de l'organisation auquel appartient l'utilisateur (valeur obtenue d'Active Directory).
- **Nombre total d'incidents**. Total d'incidents provoqués par les utilisateurs, dans l'ensemble des catégories.
- **<Nom de la catégorie>**. Nombre d'incidents provoqués par les utilisateurs pour chaque catégorie. Chaque colonne contient les données d'une catégorie.

Le rapport peut contenir les informations sur un maximum de 600 000 incidents.

RAPPORT ICP (KPI) DU SYSTEME

Le rapport ICP (KPI – Key Performance Indicators, indicateurs clés de performance) du système contient des informations sur le nombre global de messages vérifiés et ignorés, ainsi que sur le nombre de violations de stratégies dans chaque catégorie. Le rapport présente l'efficacité du Module DLP pour une période donnée.

L'en-tête du rapport contient les informations suivantes :

- **Nom du rapport**. « Rapport ICP (KPI) du système ».
- **<Date>**. Date de création du rapport.
- **<Heure>**. Heure de création du rapport.
- **Pour la période**. Période pour laquelle le rapport est créé.

Ensuite, le rapport présente deux tableaux.

Le premier tableau contient les informations suivantes :

- **Dans la zone d'application des stratégies**. Nombre de messages et pourcentage du contenu se trouvant dans la zone d'action d'au moins une stratégie. Le module DLP a appliqué les stratégies à ces messages et les a analysés.
- **Sains**. Nombre de messages et pourcentage du contenu qui, au terme de l'analyse, n'avaient violé aucune stratégie.
- **Violations**. Nombre de messages et pourcentage du contenu qui, au terme de l'analyse, avaient violé une ou plusieurs stratégies.
- **Erreurs**. Nombre de messages et pourcentage du contenu pour lesquels l'analyse n'a pas été effectuée en raison d'une erreur.

- **Temps d'attente de l'analyse**. Nombre de messages et pourcentage du contenu pour lesquels l'analyse n'a pas été effectuée en raison de l'expiration du délai d'attente de l'analyse.

- **Hors de la zone d'application des stratégies**. Nombre de messages et pourcentage du contenu ne se trouvant dans la zone d'action d'aucune stratégie. Le module DLP a ignoré ces messages sans les analyser.

Le deuxième tableau contient des informations sur le nombre de violations de stratégies par catégorie. Les lignes du tableau contiennent les noms des catégories. Le rapport indique le nombre de violations des stratégies pour chaque catégorie ainsi que la part qu'elles représentent par rapport au nombre total de violations de stratégies (en pourcentage). Le tableau inclut uniquement les catégories adaptées à une des conditions suivantes :

- des stratégies créées sur la base des catégories, une ou plusieurs violations ont été détectées durant l'exercice.

- au moment de la création du rapport, il existe des stratégies actives créées sur la base des catégories.

RAPPORT PAR STRATEGIE ET PAR INCIDENT

Le rapport par stratégie et par incident contient des informations sur le nombre d'incidents créés au cours de la période indiquée pour les violations de chaque stratégie. Les incidents sont regroupés dans le rapport par état.

L'en-tête du rapport contient les informations suivantes :

- **Nom du rapport**. « Par stratégie et par incident ».

- **<Date>**. Date de création du rapport.

- **<Heure>**. Heure de création du rapport.

- **Nombre d'incidents**. Nombre d'incidents dont les informations sont reprises dans le rapport.

- **Pour la période**. Période pour laquelle le rapport est créé.

- **Catégories**. Liste des catégories. Le rapport reprend les incidents créés conformément à ces catégories. Si le champ contient la valeur « Toutes les catégories », le rapport reprend également les incidents créés conformément aux catégories supprimées.

En dessous se trouve un tableau contenant des informations sur le nombre d'incidents créés lors de la violation de chaque politique. Ces informations sont regroupées par état d'incident. Chaque colonne contient des informations sur le nombre d'incidents portant un des états *Nouveau*, *En cours de traitement*, *Fermé (traité)*, *Fermé (faux positif)*, *Fermé (n'est pas un incident)*, *Fermé (autre)*. Le tableau reprend toutes les catégories reprises dans le rapport et toutes les stratégies créées sur la base de celles-ci.

Le rapport peut contenir les informations sur un maximum de 600 000 incidents.

CREATION D'UNE TACHE DE COMPOSITION D'UN RAPPORT

Pour créer une tâche de composition de rapport, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

2. Dans la section **Tâches de création de rapports**, appuyez sur le bouton **Nouvelle tâche** et sélectionnez le type de rapport que la tâche devra créer :

   - **Créer une tâche de rapport détaillé**.

   - **Créer une tâche de rapport par utilisateur**.

- **Créer une tâche de rapport sur les ICP (KPI) du système**.
- **Créer une tâche de rapport sur les stratégies et les incidents**.

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

3. Si nécessaire, modifiez le nom attribué automatiquement à la tâche dans le champ **Nom**.
4. Configurez les paramètres de la tâche en fonction du type de rapport créé par la tâche :
   - Détaillé (cf. section « Tâche de composition d'un rapport détaillé : configuration des paramètres » à la page 46).
   - Par utilisateur (cf. section « Tâche de composition d'un rapport par utilisateur : configuration des paramètres » à la page 48).
   - ICP (KPI) du système (cf. section « Tâche de composition d'un rapport ICP (KPI) du système : configuration des paramètres » à la page 50).
   - Par stratégie et par incident (cf. section « Tâche de composition d'un rapport par stratégie et par incident : configuration des paramètres » à la page 51).
5. Cliquez sur **OK** pour enregistrer les modifications apportées.

L'application créera le rapport conformément aux paramètres et au planning définis dans la tâche. Vous pouvez également composer un rapport à tout moment, en lançant la tâche manuellement (cf. section « Lancement d'une tâche de composition d'un rapport » à la page 53).

TACHE DE COMPOSITION D'UN RAPPORT DETAILLE : CONFIGURATION DES PARAMETRES

Pour configurer les paramètres de tâche de création de rapport détaillé, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**. Pour les tâches de création de rapports détaillés, le champ **Type de rapport** contient l'indication *Détaillé*.
2. Sélectionnez la tâche dans la liste, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans l'onglet **Principaux**, sélectionnez les incidents qui figureront dans le rapport :
   - Configurez les paramètres suivants dans le groupe **Inclure les incidents dans le rapport** :
     - **Selon toutes les catégories et stratégies**.

       L'application sélectionne pour le rapport les incidents liés à toutes les catégories et stratégies (y compris les incidents liés à des catégories et stratégies supprimées).

       Cette option est sélectionnée par défaut.
     - **Selon les catégories et stratégies sélectionnées**.

       L'application sélectionne pour le rapport les incidents créés conformément aux catégories et aux stratégies que vous avez indiquées.

       Lorsque cette option est sélectionnée, la liste des catégories et stratégies devient accessible.

       La liste contient les noms de toutes les catégories et stratégies existantes à l'heure actuelle.

       Quand une case est cochée pour une catégorie, les cases pour les stratégies créées sur la base de cette catégorie sont automatiquement cochées.

- Dans le groupe **Activer uniquement les incidents avec les expéditeurs suivants**, configurez les paramètres suivants :

  - **Tous les utilisateurs**.

    L'application sélectionne pour le rapport les incidents créés pendant l'analyse des messages envoyés par tous les expéditeurs dont les comptes utilisateur figurent dans Active Directory.

    Cette option est sélectionnée par défaut.

  - **Utilisateurs sélectionnés**.

    L'application sélectionne pour le rapport les incidents créés lors de l'analyse des messages envoyés par les expéditeurs que vous avez sélectionnés.

    Lorsque cette option est sélectionnée, la liste des expéditeurs devient accessible. Vous pouvez créer la liste à l'aide des boutons suivants :

    -  : ajouter un compte d'expéditeur à la liste à partir d'Active Directory ;
    -  : supprimer le compte de l'expéditeur sélectionné de la liste.

    Par défaut, la liste est vide.

4. Dans l'onglet **Avancés**, procédez comme suit :

- Les états des incidents s'affichent dans le champ **Inclure dans le rapport les incidents avec les états** : Les incidents portant ces états sont inclus dans le rapport. Pour modifier la sélection d'états des incidents, cliquez sur le bouton **Sélectionner** et, dans la fenêtre qui s'ouvre, cochez les cases correspondant aux états souhaités. Cliquez ensuite sur **OK**.

- Le champ **Trier les données par colonne** affiche les informations relatives aux champs utilisés pour trier les données dans le rapport et à l'ordre du tri. Pour modifier la sélection des champs, cliquez sur le bouton **Sélectionner** , puis cochez, dans la fenêtre qui s'ouvre, les champs selon lesquels le tri devra être effectué. Les boutons **Haut** et **Bas** permettent de modifier l'ordre de tri des données selon les champs. Cliquez ensuite sur **OK**.

- Configurez les paramètres d'envoi du rapport dans le groupe **Envoyer le rapport par courrier électronique** :

  - **A l'expert en sécurité de l'information**.

    Envoi d'une notification sur la violation de la stratégie à l'adresse de l'expert en sécurité de l'information.

    Si la case est cochée, l'application envoie le rapport créé à l'adresse (ou aux adresses) des experts en sécurité de l'information. L'adresse ou la liste d'adresses des experts en sécurité de l'information doit être préalablement saisie à l'entrée **Protection des données contre les fuites**.

    Si la case est décochée, l'application n'envoie pas le rapport aux adresses des experts en sécurité de l'information.

    La case est décochée par défaut.

  - **Avancé**.

    Envoi du rapport aux adresses complémentaires.

    Si la case est coché, l'application envoie le rapport créé aux adresses complémentaires indiquées dans le champ de saisie.

    Si la case est décochée, l'application n'envoie pas le rapport aux adresses complémentaires.

    La case est décochée par défaut.

5. Dans l'onglet **Planification**, configurez le mode de lancement de la tâche. Pour ce faire, configurez les paramètres suivants :

   - **Créer un rapport selon la planification**.

     Activation de la création automatique du rapport.

     Si la case est cochée, l'application crée automatiquement le rapport selon la planification établie dans la tâche.

     Si la case est décochée, le rapport n'est pas créé automatiquement.

     La case est cochée par défaut.

   - **Tous les N jours**.

     L'application exécute automatiquement la tâche à l'heure établie et selon la fréquence indiquée.

     Si cette option est sélectionnée, les champs **Tous les N jours** et **Heure de lancement**, dans lesquels vous pouvez configurer la fréquence (en jours) et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque semaine**.

     L'application lance automatiquement la tâche chaque semaine selon la planification établie.

     Si cette option est sélectionnée, les champs **Jour de lancement** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour de la semaine et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque mois**.

     L'application lance automatiquement la tâche une fois par mois, conformément au jour et à l'heure sélectionnés.

     Si cette option est sélectionnée, les champs **Jour du mois** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour du mois et l'heure de lancement de la tâche, deviennent accessibles.

6. Cliquez sur **OK** pour enregistrer les modifications apportées.

TACHE DE CREATION D'UN RAPPORT PAR UTILISATEUR : CONFIGURATION DES PARAMETRES

Pour configurer les paramètres de tâche de composition de rapport par utilisateur, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**. Les tâches de création de rapport par utilisateur affichent la valeur Par utilisateur dans le champ **Type de rapport**.

2. Sélectionnez la tâche dans la liste, puis cliquez sur le bouton **Modifier**.

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

3. Dans l'onglet **Principaux**, sélectionnez les incidents qui figureront dans le rapport :

   - Configurez les paramètres suivants dans le groupe **Inclure les incidents dans le rapport** :

     - **Selon toutes les catégories**.

     - **Selon les catégories sélectionnées**.

- Dans le groupe **Activer uniquement les incidents avec les expéditeurs suivants**, configurez les paramètres suivants :

  - **Tous les utilisateurs**.

    L'application sélectionne pour le rapport les incidents créés pendant l'analyse des messages envoyés par tous les expéditeurs dont les comptes utilisateur figurent dans Active Directory.

    Cette option est sélectionnée par défaut.

  - **Utilisateurs sélectionnés**.

    L'application sélectionne pour le rapport les incidents créés lors de l'analyse des messages envoyés par les expéditeurs que vous avez sélectionnés.

    Lorsque cette option est sélectionnée, la liste des expéditeurs devient accessible. Vous pouvez créer la liste à l'aide des boutons suivants :

    -  : ajouter un compte d'expéditeur à la liste à partir d'Active Directory ;
    -  : supprimer le compte de l'expéditeur sélectionné de la liste.

    Par défaut, la liste est vide.

4. Dans l'onglet **Avancés**, procédez comme suit :

   - Les états des incidents s'affichent dans le champ **Inclure dans le rapport les incidents avec les états** : Les incidents portant ces états sont inclus dans le rapport. Pour modifier la sélection d'états des incidents, cliquez sur le bouton **Sélectionner** et, dans la fenêtre qui s'ouvre, cochez les cases correspondant aux états souhaités. Cliquez ensuite sur **OK**.

   - Le champ **Trier les données par colonne** affiche les informations relatives aux champs utilisés pour trier les données dans le rapport et à l'ordre du tri. Pour modifier la sélection des champs, cliquez sur le bouton **Sélectionner** , puis cochez, dans la fenêtre qui s'ouvre, les champs selon lesquels le tri devra être effectué. Les boutons **Haut** et **Bas** permettent de modifier l'ordre de tri des données selon les champs. Cliquez ensuite sur **OK**.

   - Configurez les paramètres d'envoi du rapport dans le groupe **Envoyer le rapport par courrier électronique** :

     - **A l'expert en sécurité de l'information**.

       Envoi d'une notification sur la violation de la stratégie à l'adresse de l'expert en sécurité de l'information.

       Si la case est cochée, l'application envoie le rapport créé à l'adresse (ou aux adresses) des experts en sécurité de l'information. L'adresse ou la liste d'adresses des experts en sécurité de l'information doit être préalablement saisie à l'entrée **Protection des données contre les fuites**.

       Si la case est décochée, l'application n'envoie pas le rapport aux adresses des experts en sécurité de l'information.

       La case est décochée par défaut.

     - **Avancé**.

       Envoi du rapport aux adresses complémentaires.

       Si la case est coché, l'application envoie le rapport créé aux adresses complémentaires indiquées dans le champ de saisie.

       Si la case est décochée, l'application n'envoie pas le rapport aux adresses complémentaires.

La case est décochée par défaut.

5. Dans l'onglet **Planification**, configurez le mode de lancement de la tâche. Pour ce faire, configurez les paramètres suivants :

   - **Créer un rapport selon la planification**.

     Activation de la création automatique du rapport.

     Si la case est cochée, l'application crée automatiquement le rapport selon la planification établie dans la tâche.

     Si la case est décochée, le rapport n'est pas créé automatiquement.

     La case est cochée par défaut.

   - **Tous les N jours**.

     L'application exécute automatiquement la tâche à l'heure établie et selon la fréquence indiquée.

     Si cette option est sélectionnée, les champs **Tous les N jours** et **Heure de lancement**, dans lesquels vous pouvez configurer la fréquence (en jours) et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque semaine**.

     L'application lance automatiquement la tâche chaque semaine selon la planification établie.

     Si cette option est sélectionnée, les champs **Jour de lancement** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour de la semaine et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque mois**.

     L'application lance automatiquement la tâche une fois par mois, conformément au jour et à l'heure sélectionnés.

     Si cette option est sélectionnée, les champs **Jour du mois** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour du mois et l'heure de lancement de la tâche, deviennent accessibles.

6. Cliquez sur **OK** pour enregistrer les modifications apportées.

TACHE DE CREATION D'UN RAPPORT ICP (KPI) DU SYSTEME : CONFIGURATION DES PARAMETRES

Pour configurer les paramètres de tâche de création d'un rapport ICP (KPI) du système, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**. Pour les tâches de création de rapports ICP (KPI) du système, le champ **Type de rapport** contient l'indication *ICP (KPI) du système*.

2. Sélectionnez la tâche dans la liste, puis cliquez sur le bouton **Modifier**.

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

3. Configurez le mode d'exécution de la tâche. Pour ce faire, configurez les paramètres suivants :

   - **Créer un rapport selon la planification**.

     Activation de la création automatique du rapport.

     Si la case est cochée, l'application crée automatiquement le rapport selon la planification établie dans la tâche.

     Si la case est décochée, le rapport n'est pas créé automatiquement.

     La case est cochée par défaut.

- **Tous les N jours**.

  L'application exécute automatiquement la tâche à l'heure établie et selon la fréquence indiquée.

  Si cette option est sélectionnée, les champs **Tous les N jours** et **Heure de lancement**, dans lesquels vous pouvez configurer la fréquence (en jours) et l'heure de lancement de la tâche, deviennent accessibles.

- **Chaque semaine**.

  L'application lance automatiquement la tâche chaque semaine selon la planification établie.

  Si cette option est sélectionnée, les champs **Jour de lancement** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour de la semaine et l'heure de lancement de la tâche, deviennent accessibles.

- **Chaque mois**.

  L'application lance automatiquement la tâche une fois par mois, conformément au jour et à l'heure sélectionnés.

  Si cette option est sélectionnée, les champs **Jour du mois** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour du mois et l'heure de lancement de la tâche, deviennent accessibles.

4. Configurez les paramètres d'envoi du rapport dans le groupe **Envoyer le rapport par courrier électronique** :

   - **A l'expert en sécurité de l'information**.

     Envoi d'une notification sur la violation de la stratégie à l'adresse de l'expert en sécurité de l'information.

     Si la case est cochée, l'application envoie le rapport créé à l'adresse (ou aux adresses) des experts en sécurité de l'information. L'adresse ou la liste d'adresses des experts en sécurité de l'information doit être préalablement saisie à l'entrée **Protection des données contre les fuites**.

     Si la case est décochée, l'application n'envoie pas le rapport aux adresses des experts en sécurité de l'information.

     La case est décochée par défaut.

   - **Avancé**.

     Envoi du rapport aux adresses complémentaires.

     Si la case est coché, l'application envoie le rapport créé aux adresses complémentaires indiquées dans le champ de saisie.

     Si la case est décochée, l'application n'envoie pas le rapport aux adresses complémentaires.

     La case est décochée par défaut.

5. Cliquez sur **OK** pour enregistrer les modifications apportées.

TACHE DE CREATION D'UN RAPPORT PAR STRATEGIE ET PAR INCIDENT : CONFIGURATION DES PARAMETRES

Pour configurer les paramètres de la tâche de création de rapport sur les stratégies et les incidents, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**. Les tâches de création de rapport par stratégie et par incident affichent la valeur *Par stratégie et par incident* dans le champ **Type de rapport** .

2. Sélectionnez la tâche dans la liste, puis cliquez sur le bouton **Modifier**.

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

3. Sous l'onglet **Principaux**, sélectionnez les stratégies et les incidents qui seront inclus dans le rapport. Pour ce faire, configurez les paramètres suivants :

   - **Selon toutes les catégories**.

   - **Selon les catégories sélectionnées**.

4. Sous l'onglet **Avancés**, configurez les paramètres d'envoi du rapport :

   - **A l'expert en sécurité de l'information**.

     Envoi d'une notification sur la violation de la stratégie à l'adresse de l'expert en sécurité de l'information.

     Si la case est cochée, l'application envoie le rapport créé à l'adresse (ou aux adresses) des experts en sécurité de l'information. L'adresse ou la liste d'adresses des experts en sécurité de l'information doit être préalablement saisie à l'entrée **Protection des données contre les fuites**.

     Si la case est décochée, l'application n'envoie pas le rapport aux adresses des experts en sécurité de l'information.

     La case est décochée par défaut.

   - **Avancé**.

     Envoi du rapport aux adresses complémentaires.

     Si la case est coché, l'application envoie le rapport créé aux adresses complémentaires indiquées dans le champ de saisie.

     Si la case est décochée, l'application n'envoie pas le rapport aux adresses complémentaires.

     La case est décochée par défaut.

5. Dans l'onglet **Planification**, configurez le mode de lancement de la tâche. Pour ce faire, configurez les paramètres suivants :

   - **Créer un rapport selon la planification**.

     Activation de la création automatique du rapport.

     Si la case est cochée, l'application crée automatiquement le rapport selon la planification établie dans la tâche.

     Si la case est décochée, le rapport n'est pas créé automatiquement.

     La case est cochée par défaut.

   - **Tous les N jours**.

     L'application exécute automatiquement la tâche à l'heure établie et selon la fréquence indiquée.

     Si cette option est sélectionnée, les champs **Tous les N jours** et **Heure de lancement**, dans lesquels vous pouvez configurer la fréquence (en jours) et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque semaine**.

     L'application lance automatiquement la tâche chaque semaine selon la planification établie.

     Si cette option est sélectionnée, les champs **Jour de lancement** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour de la semaine et l'heure de lancement de la tâche, deviennent accessibles.

   - **Chaque mois**.

     L'application lance automatiquement la tâche une fois par mois, conformément au jour et à l'heure sélectionnés.

Si cette option est sélectionnée, les champs **Jour du mois** et **Heure de lancement**, dans lesquels vous pouvez configurer le jour du mois et l'heure de lancement de la tâche, deviennent accessibles.

6. Cliquez sur **OK** pour enregistrer les modifications apportées.

LANCEMENT D'UNE TACHE DE COMPOSITION D'UN RAPPORT

Vous pouvez lancer la tâche de composition des rapports manuellement, afin de créer un rapport quand vous le souhaitez, sans tenir compte de la programmation.

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

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**.

2. Sélectionnez la tâche dans la liste puis cliquez sur le bouton **Lancer la tâche**.

Le rapport créé apparaît dans la liste des rapports et s'ouvre dans une nouvelle fenêtre du navigateur défini par défaut dans les paramètres de votre système d'exploitation. Si l'envoi du rapport par courrier électronique est configuré dans les paramètres de la tâche, le rapport sera envoyé aux destinataires définis.

SUPPRESSION D'UNE TACHE DE COMPOSITION D'UN RAPPORT

Pour supprimer une tâche de composition d'un rapport, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   La liste des tâches apparaît dans le groupe **Tâches de création de rapports**.

2. Sélectionnez dans la liste des tâches, la tâche que vous souhaitez supprimer et cliquez sur le bouton **Supprimer**.

3. Confirmez la suppression dans la fenêtre qui s'ouvre.

La tâche sélectionnée sera supprimée.

CONSULTATION D'UN RAPPORT

Les rapports générés sont conservés dans la liste des rapports prêts et peuvent être consultés.

Pour consulter un rapport, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   Le groupe **Consultation et création des rapports** affiche la liste des rapports prêts.

2. Sélectionnez le rapport souhaité dans la liste, puis cliquez sur le bouton **Visualiser**.

Une nouvelle fenêtre du navigateur par défaut du système d'exploitation de votre ordinateur s'ouvre pour la consultation du rapport.

CREATION MANUELLE D'UN RAPPORT

Pour créer un rapport manuellement, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.
2. Dans le groupe **Consultation et création des rapports**, cliquez sur le bouton **Nouveau rapport** et sélectionnez l'option qui correspond au type de rapport à créer :
   - **Détaillé**.
   - **Par utilisateur**.
   - **ICP (KPI) du système**.
   - **Par stratégie et par incident**.

   La fenêtre **Paramètres de création du rapport** s'ouvre.
3. Configurez les paramètres du rapport en fonction de son type :
   - Détaillé (cf. section « Tâche de composition d'un rapport détaillé : configuration des paramètres » à la page 46).
   - Par utilisateur (cf. section « Tâche de composition d'un rapport par utilisateur : configuration des paramètres » à la page 48).
   - ICP (KPI) du système (cf. section « Tâche de composition d'un rapport ICP (KPI) du système : configuration des paramètres » à la page 50).
   - Par stratégie et par incident (cf. section « Tâche de composition d'un rapport par stratégie et par incident : configuration des paramètres » à la page 51).

   Les paramètres du rapport sont identiques aux paramètres des tâches de création correspondantes, à l'exception du mode d'exécution de la tâche.
4. Cliquez sur **OK** pour terminer la configuration des paramètres et créer un rapport.

Le rapport créé apparaît dans la liste des rapports et s'ouvre dans une nouvelle fenêtre du navigateur défini par défaut dans les paramètres de votre système d'exploitation. Si l'envoi du rapport par courrier électronique est configuré dans les paramètres de la tâche, le rapport sera envoyé aux destinataires définis.

ENREGISTREMENT DES RAPPORTS SUR LE DISQUE

Vous pouvez enregistrer les rapports créés sur le disque de votre ordinateur et les consulter sans la console d'administration. Vous pouvez enregistrer les rapports un par un ou en enregistrer plusieurs en même temps. Les rapports sont enregistrés sur le disque au format HTML.

Pour enregistrer un rapport sur le disque, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   Le groupe **Consultation et création des rapports** affiche la liste des rapports prêts.
2. Sélectionnez dans la liste les rapports que vous souhaitez enregistrer, puis cliquez sur le bouton **Enregistrer**.

   Si vous n'avez sélectionné qu'un rapport, la fenêtre **Enregistrer sous** apparaît. Vous pouvez nommer le fichier et choisir son dossier de destination. Si vous avez sélectionné plusieurs rapports, la fenêtre **Sélection du dossier** apparaît et vous pouvez choisir le dossier de destination.

Les rapports sélectionnés seront enregistrés dans le dossier spécifié.

SUPPRESSION DE RAPPORTS

Les rapports dont vous n'avez plus besoin peuvent être supprimés de la liste des rapports prêts. Il est possible de supprimer les rapports un à un ou par groupe.

Un rapport supprimé ne peut être récupéré.

Pour supprimer des rapports, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'entrée **Rapports**.

   Le groupe **Consultation et création des rapports** affiche la liste des rapports prêts.

2. Sélectionnez dans la liste les rapports que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.

3. Confirmez la suppression dans la fenêtre qui s'ouvre.

Les rapports sélectionnés seront supprimés.

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 antivirus :	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, Microsoft et Windows sont des marques déposées de Microsoft Corporation enregistrées aux Etats-Unis et dans d'autres pays.