SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

PLATEFORME DE GESTION DES RISQUES INTERNES

searchinform.com

1995
Création de la société

Moscow, Russia
head office

2 000 000+
d'appareils protégés par les produits SearchInform

3 000+ bureaux et partenaires dans le monde

6 produits offrent une protection complète des données contre les menaces

2019
SearchInform commence à fournir
DES SERVICES DE SURVEILLANCE

2020
Toute la gamme SearchInform peut être déployée
dans le cloud

2018-2020
Road shows
en **Amérique Latine, au Moyen-Orient et en Afrique du Nord, en Afrique du Sud, en Inde et en Indonésie**

2017
Logiciel SearchInform inclus dans le
« Gartner Magic Quadrant »

The Radicati Group
inclut SearchInform dans son étude
« Enterprise Data Loss Prevention Market, 2017-2021 »

2010
ouverture de
« Training Center »

16 programmes de formation avancée pour les spécialistes de SI

2 cours sur les bases de la cybersécurité pour les utilisateurs

PRODUITS ET SERVICES

SearchInform FileAuditor

Une entreprise moyenne stocke une énorme quantité d'informations. Certaines de ces informations sont confidentielles : données personnelles et informations financières, cahiers des charges, dessins, etc. Les informations relatives à chaque groupe sensible doivent être conservées, traitées et diffusées conformément aux règles établies.

- INFORMATIONS IMPORTANTES TOUJOURS EN VUE
- PROTECTION DES FICHIERS DANS CHAQUE TYPE D'APPLICATION

La plate-forme SearchInform fournit une PROTECTION COMPLÈTE À PLUSIEURS NIVEAUX contre les menaces de sécurité de l'information

NIVEAUX DE SÉCURITÉ DES INFORMATIONS auxquels les produits SearchInform offrent une protection

NIVEAU 1	NIVEAU 2	NIVEAU 3
Protection du système de fichiers assurée par FileAuditor, une solution de classe DCAP	Le système DLP assure une protection au niveau des postes de travail, des canaux de transmission des données et contre les risques liés au facteur humain.	Risk Monitor garantit une approche globale de la gestion des risques et de la protection des données.

*Tous les systèmes à l'intégration transparente fonctionnent sur une base technologique unique et peuvent être déployés en quelques heures. L'intégration de chaque système élargit considérablement la fonctionnalité du complexe de protection.

INFORMATIONS IMPORTANTES TOUJOURS EN VUE

SearchInform FileAuditor est une solution de la classe DCAP (Data-Centric Audit and Protection) pour un audit automatique des banques d'informations, la recherche des violations d'accès et le suivis des modifications apportées aux informations critiques. Le système protège les documents confidentiels des actions nuisibles du personnel commises par inadvertance ou intentionnellement, et en plus il nettoie le système de fichiers.

Comment FileAuditor résout le problème de surveillance de la sécurité des informations critiques :

Classification des informations sensibles

FileAuditor trouve les fichiers dans le flux de documents contenant des informations critiques et ajoute des filigranes spéciaux à chaque fichier. Le filigrane signale le type d'informations contenues dans le fichier : données personnelles, secret commercial, numéro de carte bancaire, etc.

Audit des droits d'accès

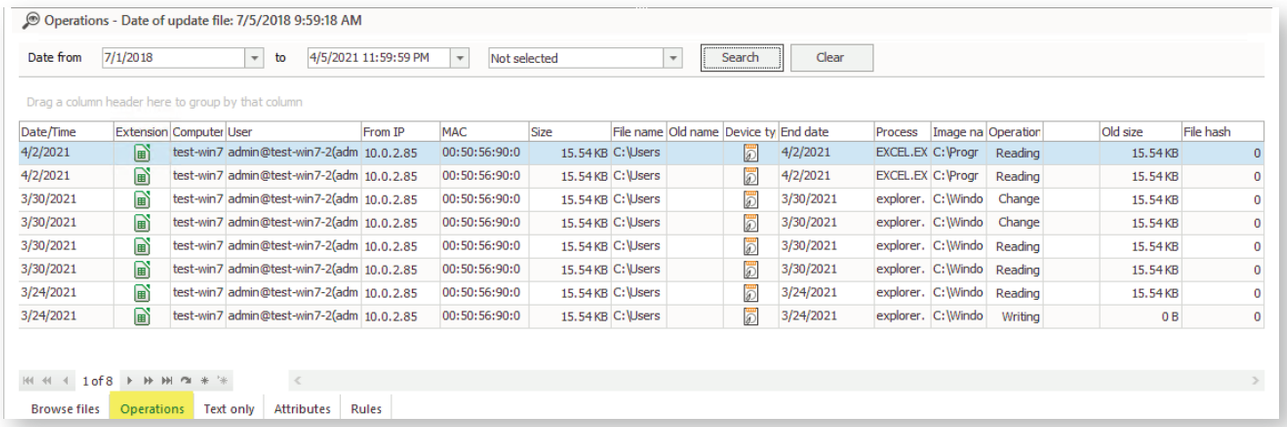
FileAuditor assure le contrôle des droits d'accès à l'information (accès complet, édition, lecture, modification, etc.) ; assure le suivi des employés sans l'accès autorisé aux données ; détecte les fichiers confidentiels stockés en violation des politiques de sécurité établies (sur un domaine public, dans des dossiers réseau partagés, sur l'ordinateur d'un employé, etc.).

Archivage des documents critiques

FileAuditor crée des clichés instantanés des fichiers critiques détectés sur un ordinateur, un serveur ou dans les dossiers réseau, enregistre l'historique de leur édition. L'archivage des informations confidentielles facilite les enquêtes sur les incidents et garantit la récupération des informations perdues.

Surveillance et blocage des actions utilisateurs

FileAuditor audite les opérations des utilisateurs avec le système de fichiers. Le personnel de la SI a toujours à portée de main les informations les plus récentes sur le cycle de vie d'un fichier (création, édition, transfert, suppression, etc.) ; bloque l'accès au fichier et son transfert dans n'importe quelle application.



Les actions avec le fichier dans Active mode

FONCTIONNEMENT DU SYSTÈME

Les informations collectées sont stockées dans une base de données, les copies des documents critiques sont enregistrées. Cela garantit que les documents restent disponibles même après la suppression.

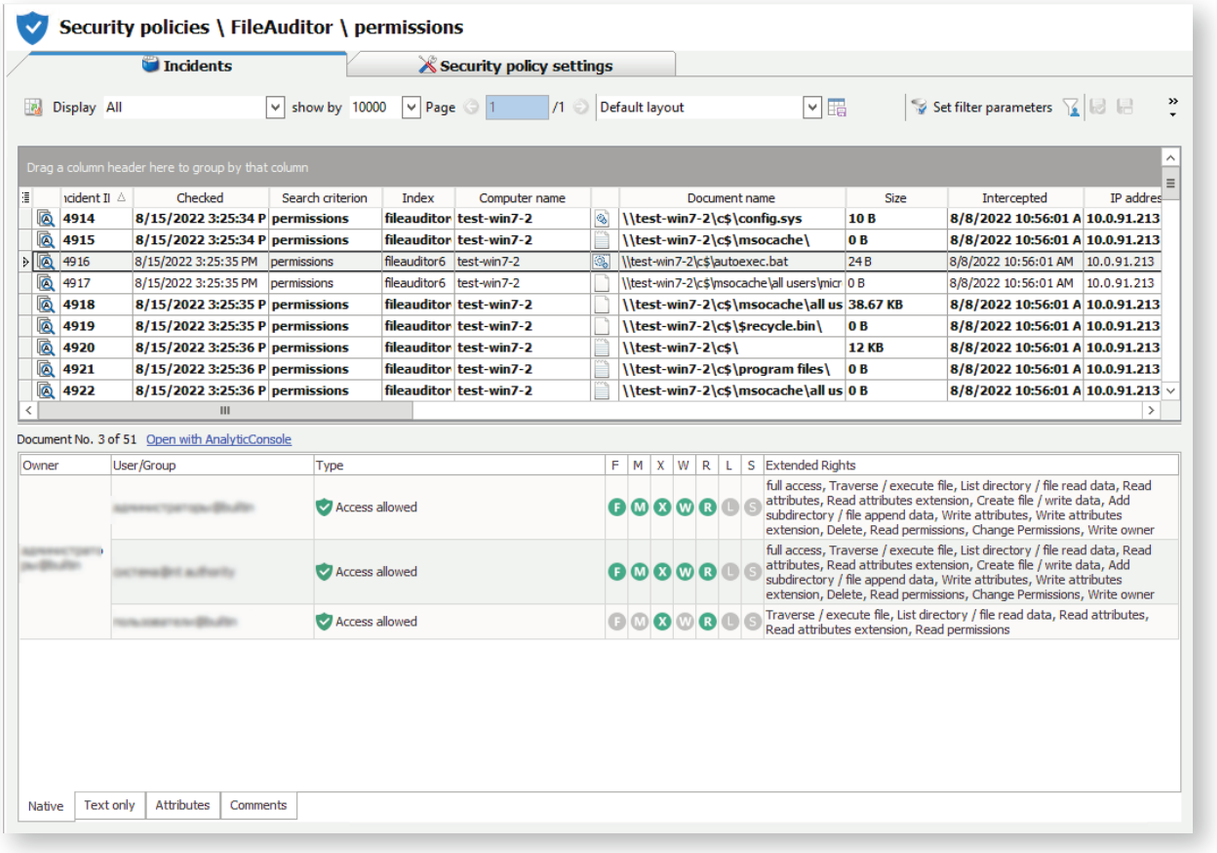
DATA ANALYSIS

Le module analytique FileAuditor visualise les résultats de l'analyse du système de fichiers conformément aux règles établies. Différents types de recherche sont disponibles dans les paramètres des règles. Les résultats de la recherche peuvent être visualisés sous forme de rapports visuels (par sources, par autorisations d'accès, par erreurs) ou sous forme d'arborescence.

Le logiciel présente :

- Arborescence des dossiers montrant les droits d'utilisateur sur chaque répertoire ou fichier.
- Opérations avec les fichiers critiques, dates de création et de modification.
- Le nombre de documents critiques sur le disque ou dans le dossier.
- Marquage de dossier (accord de confidentialité, données personnelles, rapports financiers)

Les notifications sur les violations des politiques de sécurité peuvent être générées dans AlertCenter. Par exemple, si FileAuditor détecte un document contenant des informations sensibles sur le PC d'un utilisateur qui n'a pas d'autorisation lire ce document, le responsable en sera informé automatiquement, car les notifications sont rapidement envoyées par e-mail.

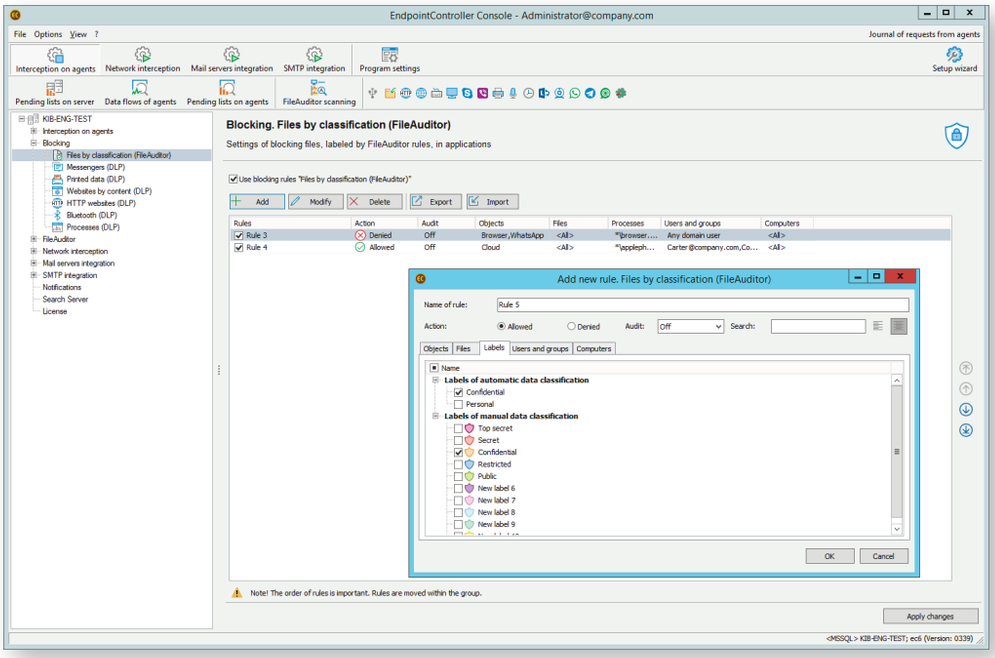


Déclenchements dans AlertCenter

Les informations collectées par les agents et le module d'analyse du réseau sont enregistrées dans une base de données Microsoft SQL Server et les copies des fichiers critiques sont stockées dans le référentiel. Grâce à cela, les documents restent accessibles même après la suppression.

DATA PROTECTION

Interdiction des opérations sur les fichiers : blocage des opérations avec accès illégal (unauthorized operations) avec les documents dans diverses applications, blocage des opérations suspectes de transfert de données et d'accès par des personnes non autorisées (access by unauthorised persons). Les commandes de verrouillage s'appliquent aux étiquettes de classification automatique et manuelle. Le système attribue des étiquettes aux fichiers en fonction de la catégorie d'informations - "secret commercial", "informations personnelles", "contrats", etc. Les autorisations et les blocages sont configurés en fonction de la classification des informations et déterminent quels utilisateurs, quels ordinateurs et quelles applications sont autorisés à interagir avec les fichiers.



Définition des règles de blocage en fonction des balises dans SearchInform FileAuditor

FileAuditor permet le blocage d'accès à un fichier dans n'importe quelle application, quels que soient sa version, son type et son origine. Les restrictions fonctionnent dans le système de fichiers où l'interdiction / l'autorisation pour les applications de lire les données est définie. Ainsi, il est possible de contrôler le processus de lecture, de modification, d'envoi de documents contenant des informations confidentielles et configurer d'autres options d'accès aux fichiers.

AVANTAGES :

- L'intégration transparente de la solution DCAP dans Risk Monitor étend considérablement la fonctionnalité du système d'atténuation des risques
- Le contrôle de la charge du PC et économie de mémoire - la surveillance peut être configurée selon un calendrier ainsi qu'être activée si un événement ou certaines circonstances se produisent ; il est possible de ne sauvegarder que les documents sensibles ; le système de duplication permet d'économiser l'espace de stockage.
- La possibilité de déployer et d'exploiter les logiciels dans le cloud. Le logiciel SearchInform peut être déployé dans le cloud, ce qui permet d'utiliser le logiciel aux entreprises qui ne possèdent pas leur propre infrastructure informatique.
- Grâce aux paramètres de règles personnalisables, les professionnels n'ont pas à travailler sur des tâches inutiles et peuvent se concentrer uniquement sur la surveillance des informations critiques.
- Les modifications apportées aux fichiers peuvent être tracées presque instantanément - le système enregistre un nombre défini de révisions de fichiers, ce qui facilite les enquêtes internes.
- Protection proactive des fichiers contre les modifications et les transferts.

SearchInform DLP

Protège l'entreprise contre les fuites d'informations confidentielles, contrôle les données au repos et les données en mouvement.

Il surveille tous les canaux de transmission de données populaires, analyse les informations, détecte et prévient les violations et fournit les rapports au service de SI.

SEARCHINFORM DLP AU SERVICE DES ENTREPRISES :

- Protège les données sensibles contre les fuites lors de l'utilisation, du stockage et du transferts.
- Contrôle des outils de télégestion et de virtualisation (TeamViewer, RAdmin, RDP).
- Facilite l'inventaire des logiciels et du matériel.
- Crypte les données afin qu'elles ne puissent pas être utilisées en dehors de l'entreprise.
- Avertit des anomalies du réseau, telles que la copie ou la suppression d'un grand nombre de fichiers.

AVANTAGES D'INTÉGRATION DU SYSTÈME DLP ET DE FILEAUDITOR.

The integration benefits:

Réduction du temps de configuration du système DLP.

Réduction du nombre des déclenchements faux positifs.

Renforcement de la sécurité de l'organisation.

Le système DLP s'intègre d'une façon transparente à FileAuditor. Les politiques de sécurité dans un système DLP sont facilement réglables en fonction des étiquettes FileAuditor.

SearchInform Risk Monitor

SearchInform propose une approche complète de la surveillance interne en étendant la solution DLP et en combinant deux concepts puissants : la prévention des incidents et la gestion des menaces internes.

Les outils de lutte contre les menaces internes et de détection des risques internes protègent votre entreprise des pertes d'argent et de réputation causées par ces incidents.

SOLUTION SEARCHINFORM DANS LE CLOUD

Les entreprises n'ont pas à choisir entre la sécurité, la commodité et le prix puisque la solution peut être déployée dans le cloud. Aucun matériel spécial n'est requis : le système collecte, traite et stocke les données dans un environnement virtuel. Ce mode de déploiement convient aux entreprises qui ne disposent pas de leur propre infrastructure informatique, dont les bureaux sont situés dans différentes villes et qui comptent de nombreux employés en télétravail.

SOLUTION ÉLARGIE :

- Détecte les incidents internes malveillants, y compris la fraude et la spéculation.
- Aide à la conformité aux exigences réglementaires et à la réalisation des enquêtes.
- Maîtrise le facteur humain et anticipe les risques RH.
- Détecte à un stade précoce les menaces potentielles ou les conditions propices aux violations et avertit des risques possibles.

Risk Monitor est un complexe automatisé de haute précision d'outils de surveillance des employés, d'évaluation des risques et d'audit interne qui garantit la conformité des politiques corporatives aux exigences régulateur et évalue le niveau de sécurité d'une entreprise par rapport aux dernières exigences réglementaires.

La solution facilite la création d'un programme de gestion des risques.

L'objectif d'un programme efficace de gestion des risques est d'examiner les opérations pour s'assurer que les résultats sont conformes aux attentes et que la réalisation des opérations est conforme au plan.

Bien que les fuites d'informations dues aux actions des utilisateurs soient souvent accidentelles, la solution SearchInform protège l'entreprise des incidents internes. Le système de gestion des risques au cœur du logiciel SearchInform aide à prévoir la fraude en entreprise et à prévenir les pertes financières.

OBJECTIFS

Collecte des informations détaillées sur les activités de l'utilisateur pour une reconstruction successive de la violation.

Garantie à l'entreprise la protection contre les risques liés au personnel et prédiction des modèles de comportement.

Création de l'archive des informations interceptées qui aide à garantir la conformité aux exigences réglementaires et renforce les politiques de sécurité nécessaires pour minimiser les risques.

Contribution à l'augmentation de l'efficacité du personnel et aide à la gestion de la loyauté dans l'équipe.

Avertissement d'une menace potentielle avant qu'un incident ne se produise, améliorant ainsi la culture de sécurité de l'entreprise et renforçant la sensibilisation aux menaces internes.

INTERCEPTION D'INFORMATIONS

La solution SearchInform est constituée de modules dont chacun contrôle son propre canal de transmission d'informations.

MailController

Intercepte les e-mails envoyés et entrants transmis dans les clients de messagerie et les services Web, y compris Gmail, Yahoo, Hotmail, etc. Enregistre l'envoi d'informations à la messagerie extra-entreprise et aux adresses e-mail des concurrents. Bloque la transmission des messages si leur contenu menace la confidentialité des informations de l'entreprise.

MonitorController

Prend les captures d'écran et enregistre les vidéos des processus actifs. Complète les photos et les vidéos avec des informations mises à jour concernant les fenêtres ouvertes et les processus actifs. Si nécessaire, affiche les informations en temps réel. Prend les photos pour identifier un intrus, reconnaît les tentatives de capture d'écran à l'aide d'un téléphone portable.

IMController

Intercepte les chats, l'historique des messages, les appels et les listes de contacts dans les messageries : Skype, Telegram, Viber, WhatsApp, Lync, Gadu-Gadu, XMPP etc. Contrôle la correspondance via les services Web dans les réseaux sociaux Facebook, Google+, LinkedIn.

ProgramController*

Collecte les données de l'activité utilisateurs sur le PC et le temps passé dans les applications, les programmes et les sites Web. Détermine automatiquement si un employé travaille ou il a ouvert le programme "pour faire semblant". Trie les ressources Web en groupes : rencontres, musique, boutiques, actualités, etc.

FTPController

Vérifie le trafic transmis par une connexion ordinaire (FTP) et sécurisée (FTPS), avertit le service de sécurité de l'information des incidents ou bloque la connexion.

HTTPController

Protège le trafic transmis via les protocoles HTTP/HTTPS. Si nécessaire, bloque le trafic Web, y compris dans les messageries Web, les services cloud, la messagerie, les blogs, les forums et les réseaux sociaux, ainsi que les requêtes de recherche. Le contrôle s'effectue même lors de l'utilisation de services d'anonymisation.

CloudController

Contrôle les fichiers téléchargés à partir de services de stockage et de partage de fichiers dans le cloud ; fichiers téléchargés et enregistrés dans les services de stockage et de partage de fichiers dans le cloud : Google Docs, Office 365, Evernote, iCloud Drive, Dropbox, Amazon S3, DropMeFiles, etc. Intercepte les fichiers envoyés et reçus via TeamViewer, RealVNC, Radmin, LiteManager.

DeviceController

Intercepte et bloque les informations transférées vers les clés USB, les lecteurs externes, les CD/DVD, via les sessions RDP et les caméras. Crypte automatiquement les données enregistrées sur la clé USB. Détecte les smartphones connectés au PC (Android, Apple, BlackBerry, Windows Phone), analyse leur contenu lorsqu'ils sont connectés en mode mémoire de masse.

Restreint l'accès des appareils au PC.

MicrophoneController

À l'aide de n'importe quel microphone détecté, enregistre les conversations au bureau et en dehors. Déclenche l'enregistrement sonore avant même que l'utilisateur ne soit autorisé dans le système - à la détection d'une conversation, aux lancement des processus et des programmes spécifiés par la politique de sécurité. Le flux audio peut être converti en texte, sur lequel les politiques de sécurité spécifiées sont également exécutées.

***** **Aide à contrôler les actions des employés en télétravail.*

Keylogger

Enregistre la saisie au clavier et les données copiées dans le presse-papiers. Permet d'intercepter les identifiants et les mots de passe et de suivre les comptes des employés sur les ressources "potentiellement dangereuses". Identifie les utilisateurs qui ont entré des mots de passe pour les documents chiffrés.

PrintController

Vérifie le contenu des documents envoyés pour impression : copie les fichiers texte, enregistre les numérisations sous forme d'empreintes digitales graphiques et de texte reconnu. Détecte les documents certifiés par un sceau, permet de contrôler l'impression de formulaires de responsabilité stricte.

CONTROL CENTER

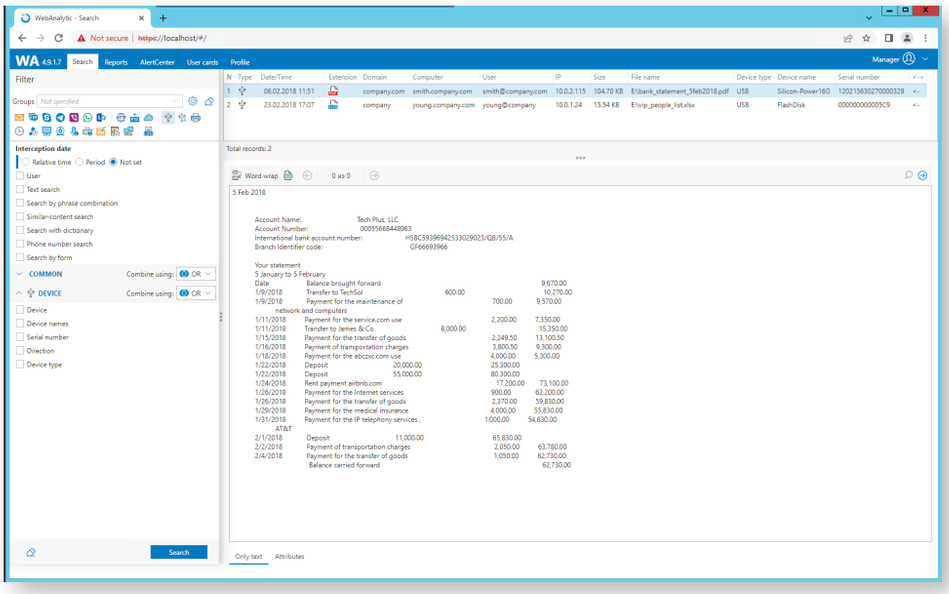
DataCenter

Gère les index et les bases de données de produits, surveille l'état du système et assure une interaction avec des systèmes tiers, comme AD, SOC, serveur de courriels sortant. Les utilisateurs de DataCenter peuvent configurer divers droits d'accès.

AlertCenter

Le « centre névralgique » du système, où les politiques de sécurité sont configurées. Un spécialiste de SI dispose de plus de 250 politiques prêtes à l'emploi qui peuvent être modifiées. Toujours dans AlertCenter, vous pouvez créer vos propres règles pour analyser les informations, configurer un calendrier de vérifications et envoyer des notifications.

Il est possible de visualiser les incidents dans la console AlertCenter sur le PC d'entreprise attribué à un employé responsable ou via une interface Web accessible depuis un ordinateur portable, une tablette, un smartphone.



Module de recherche dans la console Web SearchInform Risk Monitor

Analytic Console

Sert à la recherche et à l'analyse approfondie des données collectées, ainsi qu'à la surveillance en ligne des ordinateurs du personnel. Un spécialiste de la SI dispose de divers algorithmes de recherche et de modèles de rapport préinstallés.

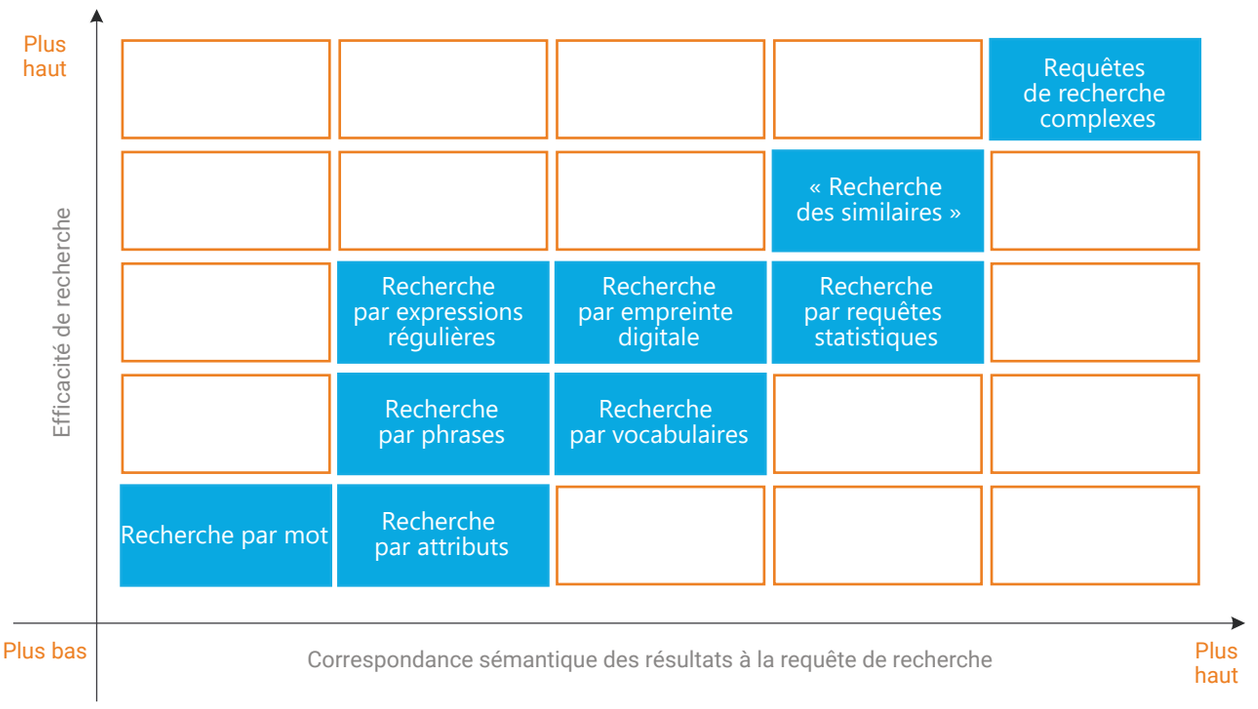
Toutes les fonctionnalités d'AlertCenter et d'Analytic Console, y compris la création de politiques, l'affichage d'incidents et de rapports et la conduite d'enquêtes, sont également disponibles via l'interface Web. Cela rend la protection mobile.

CAPACITÉS ANALYTIQUES

Pour le travail efficace du service de SI, une interception complète par tous les canaux, ainsi que la recherche correcte des informations collectées et leur analyse sont nécessaires. Un puissant module d'analyse, une variété de types de recherche, une analyse automatisée des graphiques et de l'audio permettent à un spécialiste de la SI de contrôler plusieurs milliers d'employés.

Analyse de texte

Une variété d'algorithmes permet une vérification approfondie des messages texte et des documents. Parmi les technologies de recherche, il en existe des uniques. Par exemple, l'algorithme breveté d'analyse sémantique "Recherche des similaires". Il détecte les documents sensibles, même s'ils ont été modifiés, de sorte que les résultats de la recherche incluront les documents similaires non seulement "techniquement" mais aussi par leur sens. La recherche de requêtes complexes combine plusieurs algorithmes en liant des requêtes simples avec des opérateurs logiques "ET", "OU" et "NON".



Analyse graphique

Le système détermine et catégorise les types d'images circulant dans l'entreprise - PDF, photos, copies scannées. Le système OCR (système de reconnaissance de caractères) intégré détecte les documents qui correspondent aux modèles spécifiés : passeports, cartes bancaires, permis de conduire, etc. La technologie permet de trouver des données personnelles, financières et toutes autres données sensibles dans les archives, même si elles ont été transmises sous forme de documents numérisés.

Analyse audio

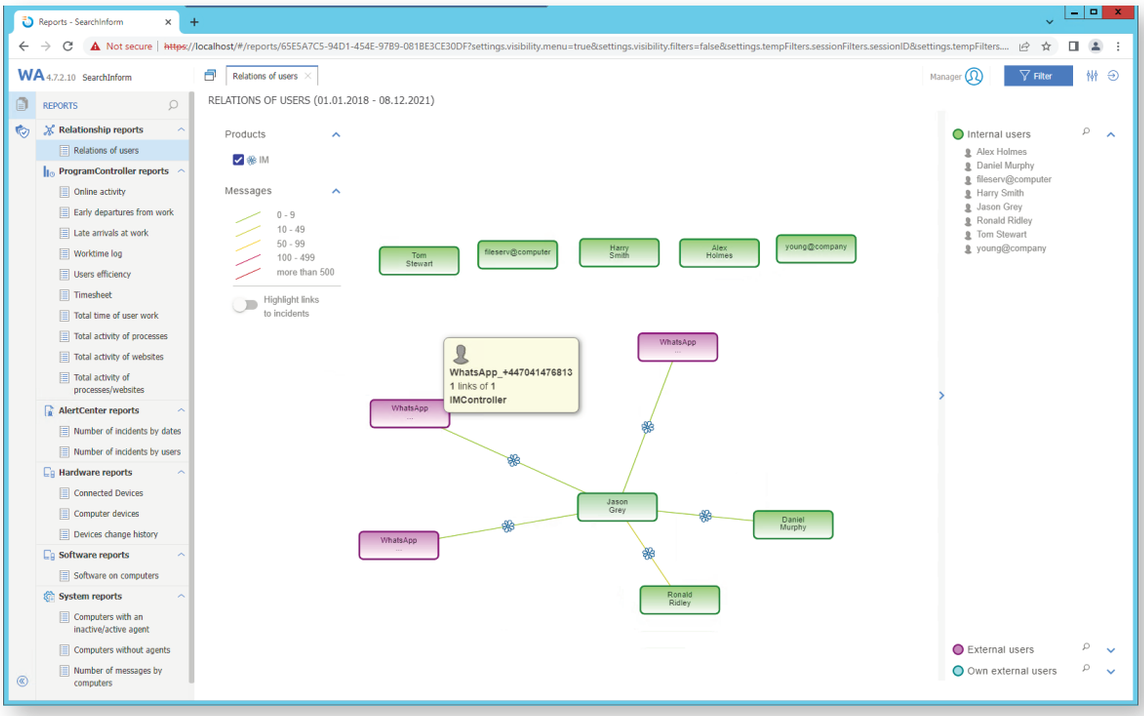
La solution SearchInform convertit les enregistrements audios interceptés en texte et vérifie la conformité du texte décrypté aux politiques de sécurité. L'enregistrement des conversations est activé lorsque la parole est détectée ou lorsque les processus et programmes spécifiés par la politique de sécurité sont lancés.

RAPPORTS&UEBA

Le logiciel SearchInform visualise tous les événements et communications au sein de l'entreprise via les rapports - dans Analytic Console et l'interface Web. TIl existe plus de 30 modèles de base dans le système. L'assistant de rapport vous permet de créer votre propre rapport, non limité par des critères.

Rapport sur les relations utilisateurs

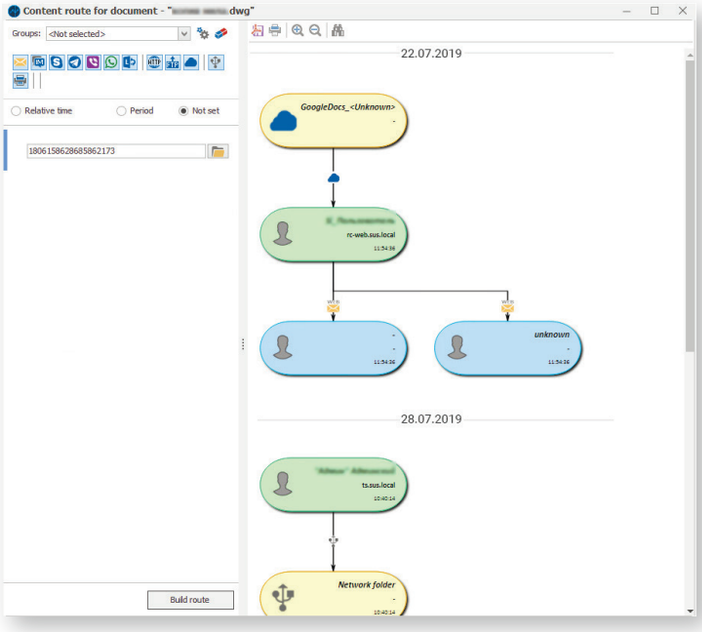
Affiche les liens de communication entre les employés et avec les destinataires externes sous forme d'un graphique des relations. Permet de voir l'activité des utilisateurs sur tous les canaux de communication ou sur une ligne de communication sélectionnée. Facilite les enquêtes internes.



Graphique des relations construit dans la version Web de l'Analytic Console

Rapport sur le déplacement de fichier

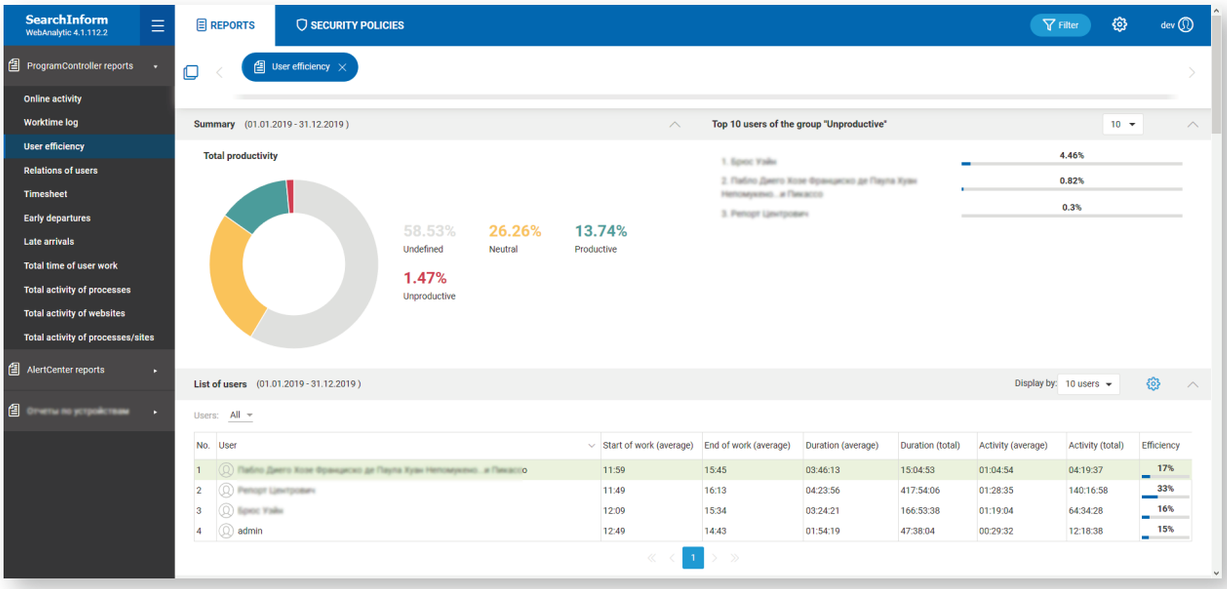
Rend transparent le mouvement du document de l'expéditeur au destinataire via les canaux de communication internes et externes. Permet d'établir rapidement l'auteur du document, la source et les moyens de diffusion de l'information.



Itinéraire de contenu

Rapport sur les performances de l'utilisateur

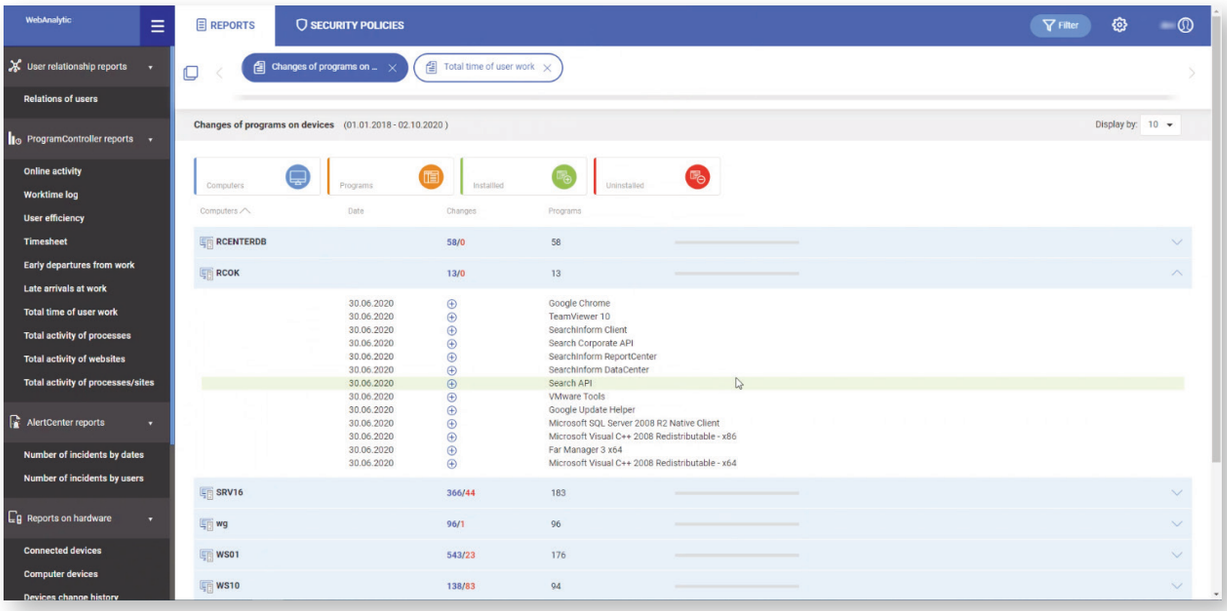
Reflète la productivité globale des employés de l'entreprise sous forme de graphiques et de ratings. Fixe la fréquence des départs et arrivées en avance, le nombre de retards. Visualise les performances des utilisateurs pendant la semaine de travail dans un format de calendrier.



Rapport sur les performances de l'utilisateur

Rapport sur les programmes et les appareils (hardware)

Signale toute modification apportée au matériel installé et aux appareils connectés. Cela facilite l'inventaire et protège contre le vol ou le remplacement non autorisé de l'équipement. Les rapports sur les logiciels structurent les données concernant les activités d'installation et de suppression de logiciels.

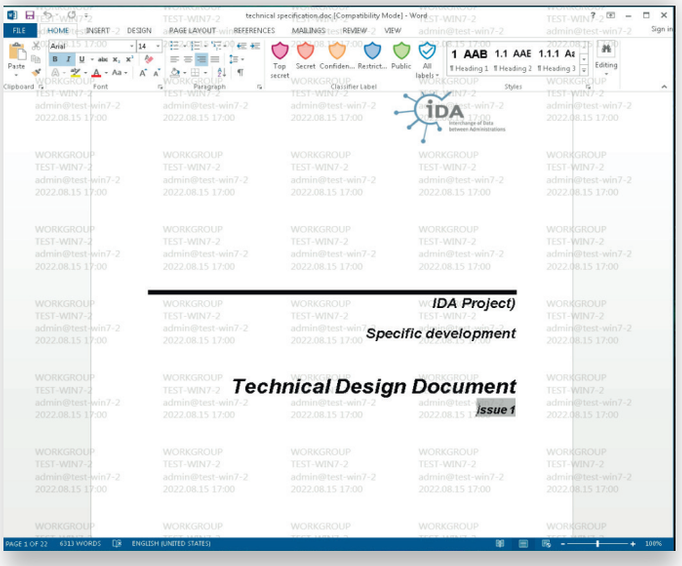


Rapport sur les programmes et les appareils

CONTRÔLE ET ENQUÊTE

Détection des fuites effectuées à l'aide de captures d'écran ou en photographiant le moniteur

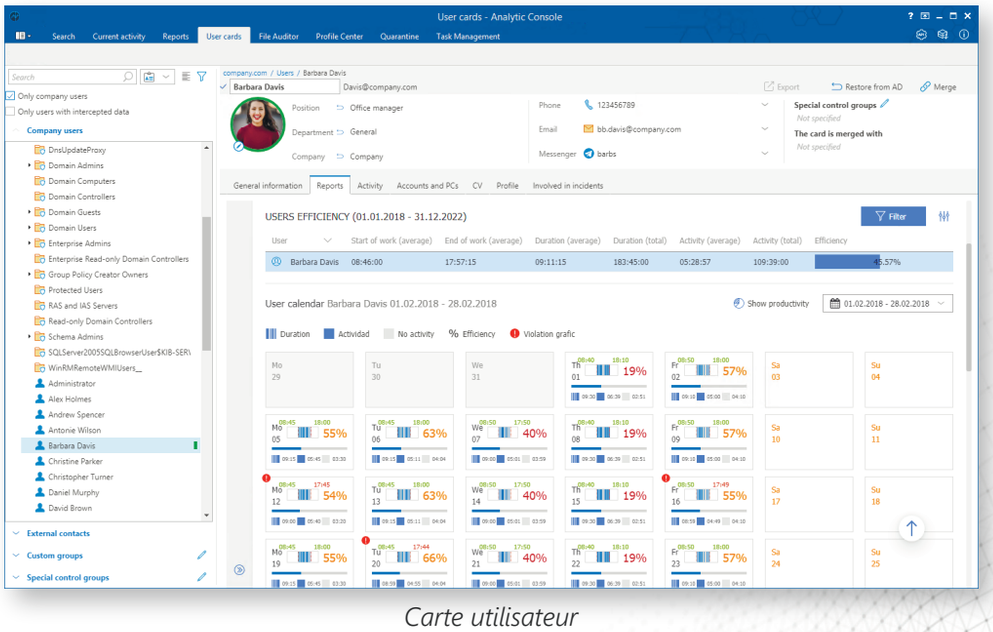
Trouver la source d'une fuite lorsqu'un utilisateur prend des captures ou des photos d'écran est une tâche extrêmement difficile. Grâce à SearchInform Risk Monitor et à l'outil (intégré) d'ajout des filigranes, cette tâche devient beaucoup plus facile. Lorsqu'on fait une capture d'écran ou on prend une photo d'écran d'un ordinateur protégé, la recherche dans des ressources externes permet au professionnel de la SI d'identifier facilement une source de fuite. Le filigrane contient une identification de l'ordinateur et de l'employé qui l'exploite.



Filigranes crées par SearchInform Risk Monitor

Carte utilisateur

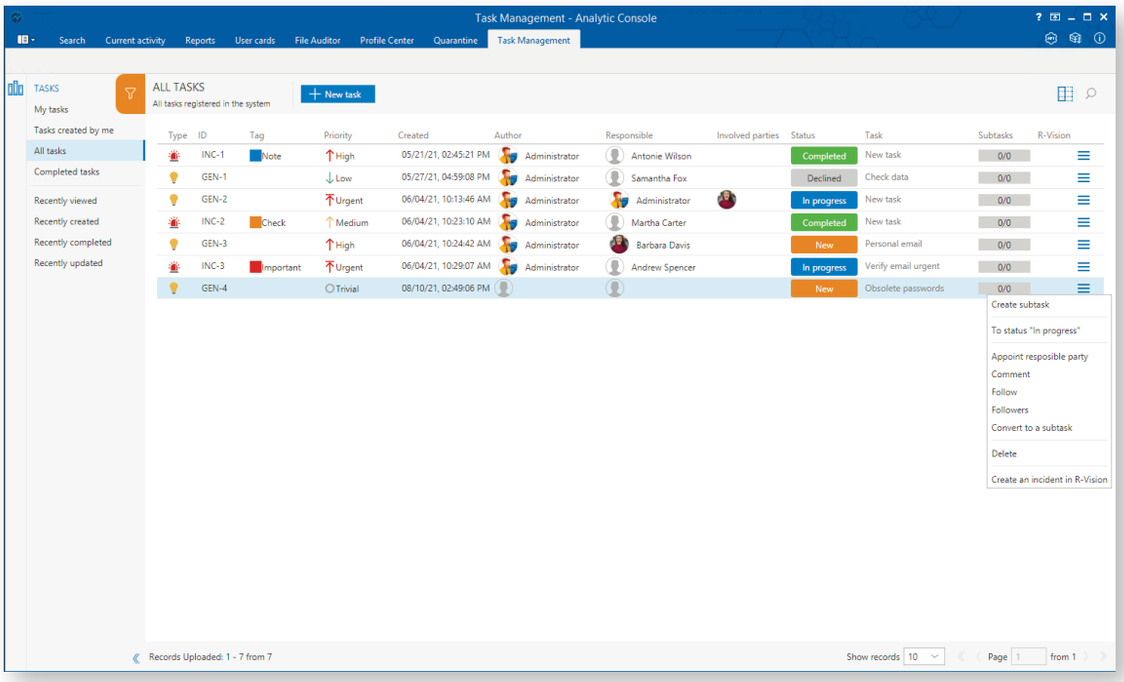
La carte utilisateur recueille un "dossier" sur chaque employé(e), reprenant automatiquement tous les incidents dans lesquels il/elle a été impliqué(e). La carte utilisateur contient les rapports individuels, la biographie et les coordonnées de l'employé, son historique d'emploi.



Carte utilisateur

Gestion du processus d'enquête

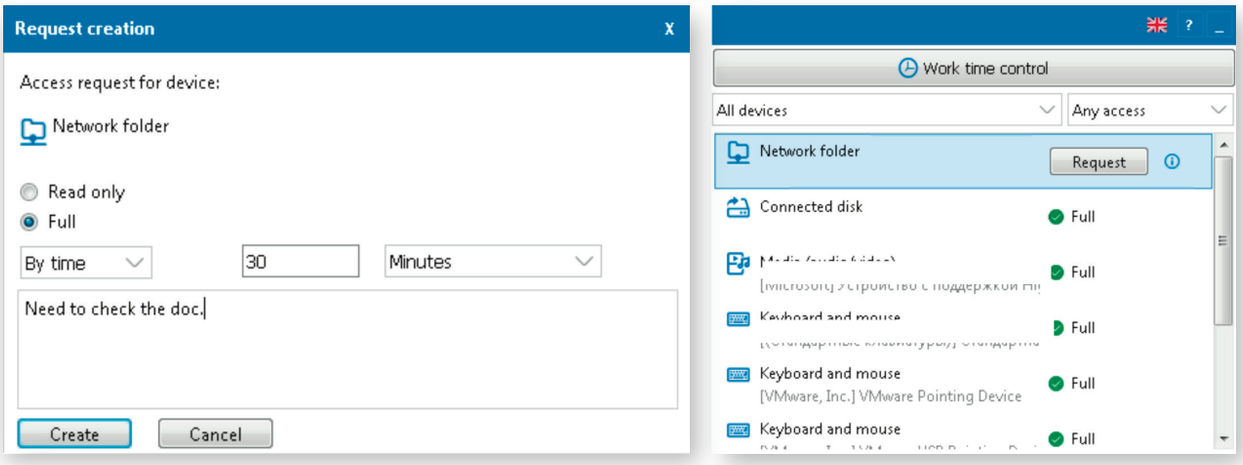
Task Manager sert à coordonner les actions des spécialistes de la SI. TCet outil permet de répartir les tâches, de suivre l'avancement des enquêtes et de créer des rapports sur leurs résultats - y compris leur transfert au SOC.



Outil Task Management

Interface utilisateur

Informe les employés des contrôles de temps de travail, ainsi que des décisions actives ou des accès refusés. L'interface utilisateur permet d'envoyer directement au service de SI les demandes d'utilisation des clés USB et d'autres appareils. Le spécialiste de SI peut émettre les autorisations pour la période demandée, modifier la période d'accès ou révoquer l'autorisation pendant la session si un incident est suspecté.



Interface utilisateur sur l'agent

Le mode de gestion "ouvert" utilisant l'interface sur les PC des utilisateurs discipline des employés et réduit la charge du service de SI.

UNIQUE FEATURES

1 Unique analytical features unavailable in any other tool

Fonctionnalités analytiques uniques indisponibles dans d'autres outils. En plus des fonctionnalités analytiques pratiques comme la recherche avec le dictionnaire, les expressions régulières, les empreintes digitales numériques et OCR, SearchInform Risk Monitor propose des fonctionnalités telles que la recherche d'images similaires à l'original, la recherche dans tous les enregistrements audio (à l'aide de la technologie de conversion audio-texte) et la recherche de contenu dans les enregistrements vidéo des actions de l'utilisateur, ce qui permet de vérifier uniquement les actions qui vous intéressent.

2 Des outils d'investigation performants dans une seule solution

Le produit permet d'effectuer un enregistrement audio et vidéo des actions de l'utilisateur, de capturer toutes les actions de l'utilisateur avec les fichiers ou les dossiers, les journaux d'audit, les appareils ou les logiciels, ainsi que de suivre les contrevenants via des canaux audio et vidéo en temps réel.

3 Contrôle de l'efficacité de travail des utilisateurs

SearchInform Risk Monitor évalue automatiquement les performances des employés dans diverses applications et sites Web. Cette fonctionnalité permet de renforcer la discipline dans l'entreprise et de détecter les problèmes existants avec les processus métier.

4 Stabilité du système sous charge, confirmée par la pratique

Parmi les clients de SearchInform, il y a de très grandes entreprises de secteurs différents, ce qui confirme le fonctionnement stable du système dans une grande variété d'environnements informatiques et sous une charge élevée.

5 Possibilité d'étendre la fonctionnalité grâce aux produits du même fabricant

SearchInform propose une suite de produits comprenant Risk Monitor, DLP, SIEM et FileAuditor (solution DCAP). Tous les systèmes fonctionnent sur une base technologique unique. A l'intégration transparente, ils peuvent être déployés en quelques heures.

6 Multiplateforme et accessibilité depuis n'importe quel appareil

L'interface utilisateur de SearchInform Risk Monitor est disponible en deux options - en tant que client Windows et en version.

AVANTAGES

Itinéraire de transfert du document

Montre le mouvement des documents, indique l'expéditeur et le destinataire, ainsi que les canaux utilisés pour le transfert de données.

Possibilité de déploiement dans le cloud

Tous les composants de Risk Monitor peuvent être déployés sur une plateforme cloud (de SearchInform ou d'un autre fournisseur) sans compromettre la fonctionnalité du système. Ce format de protection des données permet de faire les économies sur l'achat et la maintenance du matériel.

Possibilité de contrôle des outils d'accès à distance

Les solutions SearchInform protègent les informations transmises via des environnements virtuels et des logiciels d'accès à distance. La surveillance s'effectue au niveau du presse-papiers, de la connexion des lecteurs virtuels, ainsi qu'au niveau des fonctionnalités des programmes (par exemple, le transfert via le menu contextuel TeamViewer).

Service de mise en œuvre et Centre de formation

La collaboration avec plus de 3 000 entreprises de différents secteurs permet de créer rapidement les packs uniques de politiques de sécurité focalisés sur les tâches primordiales et les spécificités du métier du client.

Possibilité de déployer rapidement des logiciels sans avoir à modifier la structure du réseau

Les informaticiens du client pourront installer la solution SearchInform en quelques heures. Le processus d'installation n'interfère pas avec le fonctionnement des systèmes d'information locaux de l'entreprise.

Surveillance des données au repos

Le système signalera des faits enregistrés de présence d'informations confidentielles là où elles ne devraient pas être.

Intégration avec d'autres produits SearchInform

La solution SearchInform s'intègre de manière transparente à SIEM, ProfileCenter, FileAuditor, ce qui améliore le niveau de protection des informations et de sensibilisation aux risques, réduit le temps de réponse à un incident et permet de faire une enquête complète des violations.

Outils d'enquête successive sur les incidents

Des outils de surveillance de l'activité en ligne comme l'enregistrement des conversations et le suivi des saisies en temps réel, le suivi des saisies au clavier et la création de vidéos par webcam, les flux d'informations, les graphiques de liens et les cartes utilisateurs, la gestion des tâches du service de SI, la recherche automatisée des incidents - aideront à reconstruire progressivement les failles de sécurité.

Éléments d'intelligence artificielle

Le système reconnaît automatiquement les visages des utilisateurs et aide à savoir si le PC n'est pas exploité par son propriétaire. Il enregistre les tentatives de photographier un écran d'ordinateur avec un smartphone et protège les prises de vue par des filigranes uniques pour identifier la source de la fuite.

Protection proactive contre les incidents

Risk Monitor réalise un blocage intelligent en fonction du contenu pour tous les canaux de contrôle - les utilisateurs ne pourront pas transférer les fichiers et les messages au contenu confidentiel. L'interface de l'agent avertira l'utilisateur d'une violation accidentelle et inculquera une culture de sécurité de l'information.

Module d'analyse puissant

Offre une solution rapide et flexible pour la mise en place d'alertes et pour l'analyse des flux de données sans avoir besoin de faire appel à des spécialistes externes. Grace aux produits SearchInform, un spécialiste peut contrôler le travail de plusieurs milliers d'employés.

SearchInform TimeInformer

La présence d'un salarié au travail ne garantit pas nécessairement qu'il accomplira ses fonctions. Les employés prennent souvent des pauses, pauses-cigarette et pauses-café, discutent avec des collègues, utilisent les médias sociaux, arrivent en retard ou partent plus tôt.

ACTIVITÉ D'ÉQUIPE

TimeInformer is an employee monitoring solution that protects business from inefficient work and financial losses related to personnel.

TimeInformer analysera les ordinateurs de service et aidera à déterminer :

Les contrevenants à la discipline du travail qui sont en retard, partent tôt, prennent souvent des pauses/pauses cigarette et pauses café.

Les freelances qui effectuent des tâches annexes pendant les heures payées par l'entreprise.

Les fainéants qui discutent, font des achats en ligne, sont distraits par des jeux et d'autres activités.

Les employés insatisfaits qui dressent leurs collègues contre l'employeur et ceux qui sont « burn out » en raison de tâches ennuyeuses ou d'une charge professionnelle trop élevée.

Le programme détermine le temps de travail ou d'oisiveté des employés, montre avec quels programmes et sites ils travaillent, identifie les sites de rencontres, les boutiques en ligne, les actualités, les séries. Et évalue l'efficacité réelle du personnel en fonction des paramètres déterminés.

CONTRÔLE EN TEMPS RÉEL

TimeInformer peut être utilisé non seulement en mode arrière-plan. Le programme se connecte aux moniteurs et aux microphones du PC et reproduit en temps réel ce qui se passe sur les écrans du PC et dans la zone de la portée du microphone.

En mode en ligne, vous pouvez enregistrer des négociations importantes avec les partenaires et clients clés. Et aussi voire l'activité réelle de l'employé sur le PC pendant une certaine période de temps. Le service SI peut surveiller jusqu'à 16 ordinateurs simultanément.

Le service SI peut surveiller jusqu'à 16 ordinateurs simultanément. TimeInformer peut être déployé dans le cloud. Cette option ne nécessite pas de frais supplémentaires pour l'achat et la maintenance du matériel.

AIDE À LA DÉCISION MANAGÉRIALE

Le programme propose 33 modèles de rapport disponibles qui aideront à détecter les contrevenants et à modifier la charge de travail des employés afin que vos objectifs professionnels soient atteints.

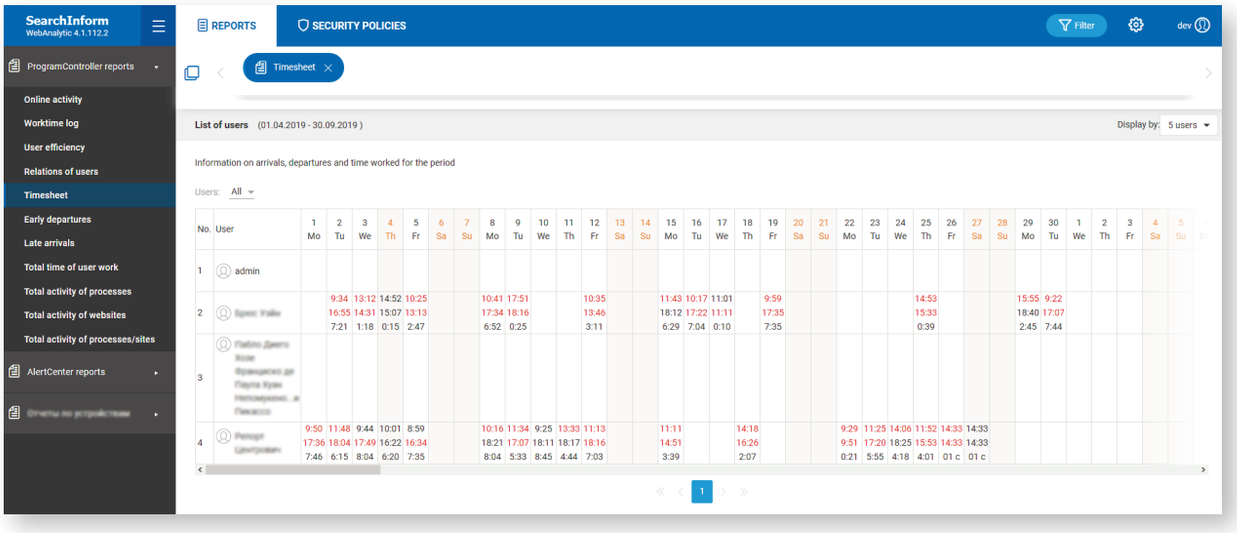
Dans TimeInformer les groupes de rapports suivants sont disponibles :

- par activité des utilisateurs dans les applications et sur les sites Web ;
- par programmes avec un historique d'installation et de suppression de logiciels ;
- par appareils avec des données concernant les équipements installés sur le PC et les modifications de leur configuration.

Les rapports et les notifications sont personnalisables. Le système envoie automatiquement des alertes sur les violations critiques.

CONFORT D'UTILISATION

Grâce à l'interface Web, vous pouvez contrôler votre personnel à l'aide de TimeInformer partout dans le monde. Les droits d'accès aux rapports et aux fonctions administratives sont différenciés par les tâches et les responsabilités du poste. Au souhait, des notifications automatiques sur les activités suspectes des employés peuvent être reçues par e-mail.



Feuille de temps de travail dans l'interface web

AVANTAGES

- Protection contre l'auto-suppression du PC et notification sur telles tentatives ;
- Contrôle des employés en télétravail ou en mission professionnelles ;
- Interface web donnant accès aux résultats de suivi en dehors du bureau
- Possibilité d'intégration avec CIB, qui aide aux enquêtes internes

SearchInform SIEM

- LE PREMIER SIEM "PRET A L'EMPLOI"
- CRÉATION DES RÈGLES DE CORRÉLATION EN 2 CLIC

L'infrastructure informatique de l'entreprise se compose de nombreux systèmes : pare-feu, systèmes d'exploitation, serveurs de messagerie, bases de données et périphériques réseau.

Beaucoup de ces systèmes sont des sources de données qui intéressent les attaquants et, de ce fait, nécessitent une protection spéciale.

Contrôle automatique des événements de sécurité

SearchInform SIEM est un système de gestion des événements de sécurité de l'information en temps réel qui aide à identifier et à répondre aux incidents de SI. Il accumule des informations provenant de diverses sources, les analyse, enregistre les incidents et en informe le service de SI.

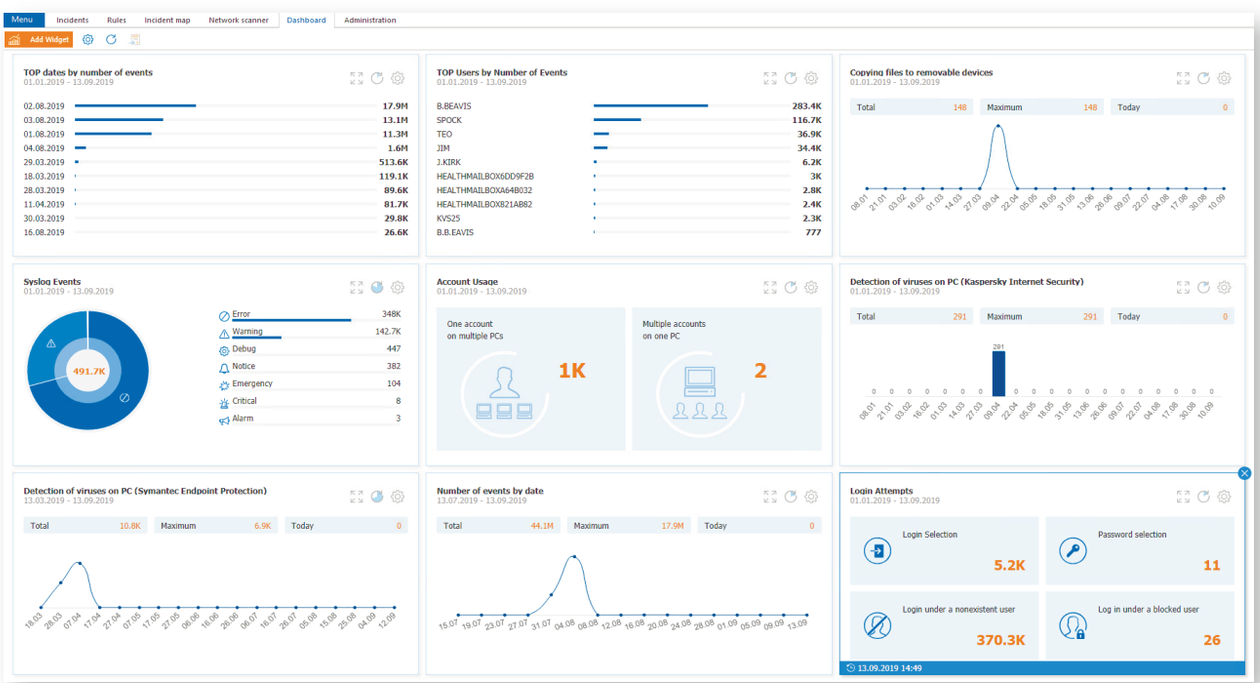


Tableau de bord avec statistiques d'événements

SearchInform SIEM détecte :

- Épidémies de virus et cas particuliers
- Tentatives d'accès aux données non autorisé
- Attaque par martellement
- Comptes actifs non-supprimés des employés licenciés.
- Défauts de configuration du matériel
- Non-respect du régime thérmique autorisé pour le fonctionnement du materiel
- Suppression des informations des ressources critiques
- Utilisation des ressources de l'entreprise en dehors des heures d'ouverture
- Suppression des machines virtuelles et des snapshots
- Connection des nouveaux équipements à l'infrastructure informatique
- Modification des politiques de groupe
- Utilisation de TeamViewer, accès à distance aux ressources de l'entreprise
- Événements critiques dans les moyens de protection
- Autres erreurs et défaillances dans le fonctionnement des systèmes informatiques

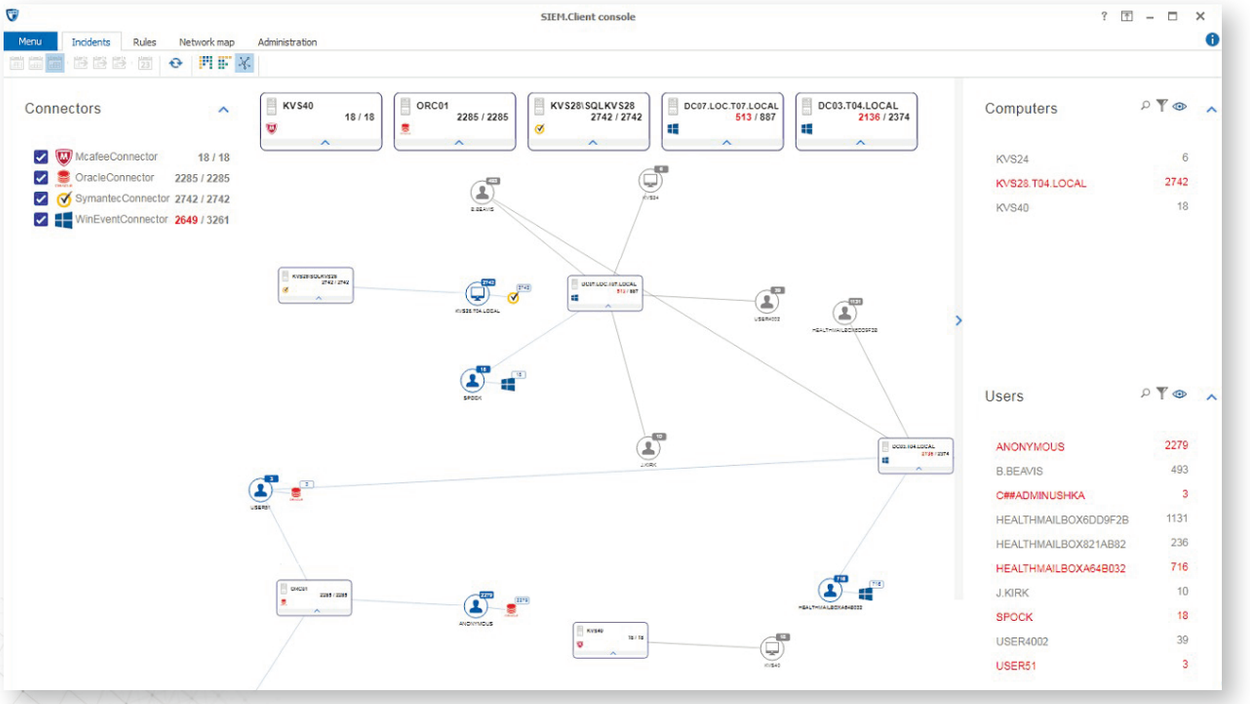
RÈGLES DE CORRÉLATION PRÉDEFINIES

Après l'installation du système, le service de SI a accès à plus de 300 règles de corrélation prêtes à l'emploi qui identifient les incidents. Les utilisateurs peuvent modifier et personnaliser les règles existantes et en créer des uniques, sélectionner des sources dans une liste prédéfinie et connecter leurs propres (la fonction "connecteur personnalisé").

Les règles de corrélation prêtes à l'emploi utilisent les sources de données suivantes :

- système d'exploitation ;
- serveurs de messagerie ;
- contrôleurs de domaine et postes de travail ;
- serveurs et postes de travail Linux ;
- SGBD ;
- systèmes DLP ;
- serveurs de fichiers ;
- environnements de virtualisation ;
- antivirus;
- pare-feu et dispositifs de sécurité réseau de bout en bout
- solutions sur la plate-forme 1C ;
- autres sources de journal système.

Pour rechercher des incidents dans un groupe d'événements provenant de différentes sources, il est possible de configurer les règles de corrélation croisée.



Incident display screen

Règles de corrélation prédéfinies SearchInform SIEM :

Pour les serveurs de messagerie

- Accès à la boîte e-mail par un non-propriétaire
- Changement de propriétaire d'une boîte e-mail
- Autorisation d'accès à la boîte e-mail

Pour les contrôleurs de domaine et des postes de travail

- Activation/ajout temporaire d'un compte
- Un compte sur plusieurs PC
- Martellement et mots de passe périmés

Pour environnement de virtualisation

- Événements de connexion/déconnexion pour VWview/VMware
- Mots de passe erronés
- Suppression de snapshot

Pour accéder aux ressources de fichiers

- Accès aux ressources critiques
- Octroi temporaire de droits sur un fichier/dossier
- Grand nombre d'utilisateurs travaillant avec un fichier

FONCTIONNEMENT DU SYSTÈME

1 Collecte des événements provenant de diverses sources logicielles et matérielles : équipements réseau, logiciels, outils de sécurité, système d'exploitation.

2 Analyse les événements et génère des incidents conformément aux règles, détecte les menaces en identifiant les relations (corrélations, y compris les corrélations croisées) des événements et/ou incidents.

3 Automatiquement avertit les personnes responsables des incidents.

4 Normalise et détaille les incidents pour une enquête plus approfondie : détermine le type, la source de l'incident, lorsqu'il est intégré à AD-utilisateur susceptible d'être impliqué dans l'événement.

AVANTAGES

- Mise en œuvre rapide sans longue pré-configuration (le logiciel peut être mis en service en une journée). Résultats dès le premier lancement.
- Facilité d'utilisation : un employé sans compétences en informatique peut gérer le programme, car il n'y a pas besoin de connaître les langages de programmation pour créer des règles de corrélation et de corrélation croisée.
- Faibles exigences pour le matériel, licences claires, coût de possession confortable.
- Analyses prêtes à l'emploi : le système est livré avec un ensemble de règles prédéfinies et prend en compte l'expérience et les tâches des entreprises de tous les domaines d'activité et secteurs économiques.
- Gestion des incidents. Création d'une enquête basée sur un ou plusieurs incidents.

L'intégration transparente avec Risk Monitor augmente le niveau de sécurité des informations de l'entreprise et permet d'enquêter pleinement sur l'incident et de collecter des preuves.

Services

SearchInform fournit les services aux entreprises qui ne disposent pas d'un département de gestion des risques dédié ou qui ne disposent pas de suffisamment de ressources pour mettre en œuvre et maintenir
de manière indépendante les systèmes de protection et de surveillance des données.

Nos services permettent à l'entreprise de profiter d'une solution qui nécessite des coûts financiers et de main-d'œuvre minimaux sans besoin d'embaucher de spécialistes. Le client reçoit le système avec une équipe d'analystes possédant une énorme expérience dans ce domaine. Les spécialistes commencent à travailler immédiatement après le déploiement du système sans leurs intégration dans les effectifs, ni prise en charge de congés, arrêts de maladie et frais de formation.

Pour chaque produit SearchInform, l'option As-a-Service est disponible. Tous peuvent être déployés dans le cloud, ce qui permet d'économiser les finances de l'entreprise, car ils ne nécessitent pas d'investissement pour l'équipement et la maintenance.

Nom du produit	Possibilité d'externalisation ?	Possibilité de déployement dans le cloud ?
SearchInform DLP	+	+
SearchInform Risk Monitor	+	+
SearchInform FileAuditor	+	+
SearchInform SIEM	+	+
SearchInform TimeInformer	+	+

COMMENT CELA FONCTIONNE ?

Le spécialiste configure le système en fonction des tâches du client.

Le client bénéficie d'une autorité maximale dans le système.

A la détection d'un incident, le spécialiste contacte le client (le mode de communication est convenu à l'avance).

Le spécialiste fournit au client des rapports sur les incidents pour la période sélectionnée (une fois par jour/semaine/mois).

Le client peut travailler dans le système avec un spécialiste ou d'une façon autonome.

Le client peut fixer au spécialiste des tâches concrètes.

OBJECTIF – SOLUTION

Nos services permettent d'identifier les points faibles de l'entreprise en peu de temps (les premiers résultats sont obtenus dans un délai de 1 à 3 mois).

Un spécialiste qui travaille avec le client contrôle l'étape de déploiement du programme et prend également des décisions de gestion en fonction des résultats des rapports reçus et des incidents ayant fait l'objet d'une enquête.

Summary report on the incidents. Details on each incident are availble in the folder with the incident number.

No.	Date	Employees related to the incident	Incident overview	Comment	Link to documents
			Confidential data		
1		Employee name	Copied some databases with name 'BASE C1' to USB drive.	It is not clear why the employee copied some strange	Link+RCI-
2		Employee name	Copied files in .cnc format to USB drive. The files appear to be some programs for machine tools.	The question is why.	Link
3		Employee name	Copied corporate documents to flash drive.	Not clear why the employee did it.	Link
4		Employee name	Copied a file with the name 'Efficiency' to USB drive.	Not clear why the employee did it.	Link
5		Employee name	Numerous corporate documents were copied to USB drive.	Not clear why the employee did it.	Link
			Job search		
6		Employee name	Chatted with a friend on Facebook on her plan to leave the current job in her native town and find a job in Moscow.	Job search.	Link
7		Employee name	The employee's receiving e-mails from hh.com with recommended vacancies and CV views.	Job search.	Link
8		Employee name	On Facebook sent a CV of her husband, emloyee of the same company, to her daughter.	Probably, to be sent to a would-be employer.	Link
			Forgery of documents		
9		Employee name	Forgery of documents in Paint.	Set a client's stamp and signature on the specification.	Link
10		Employee name	Edition of the corporate stamp in Photoshop.	Not clear why the employee did it.	Link
11		Employee name	Forgery of documents in Paint.	Stamped the specification document.	Link
			Side companies		
12		Employee name	Downloaded from GoogleDocs various invoices, payment documents in which there were specified different company names. All of them were headed by Employee 12.	Side company.	Link
			Discussion of the management		
13		Employee name	In Paint, was drawing on the director's photo.	Mocking the management.	Link
14		Employee name	Discussion of the management on Facebook.	Discussion of the management.	Link
15		Employee name	In the correpsosnde on WhatsApp, was discussing the director mentioning one manager.	Discussion of the management.	Link
			Big-budget purchases		
16		Employee name	The employee had correspondence with a project developer about participation interest in buying a flat.	Discussed flat payment terms.	Link
17		Employee name	Printed out an apartment equity construction agreeemnt.	The agreement included sums of money of own participation and credit amounts.	Link
			Entrepreneurship and side jobs		
18		Employee name	Documents sent to a cloud storage made it clear that the employee was a independent entrepreneur and provided services, including to the company he worked in.	Likely to have side job damaging the current company.	Link
19		Employee name	Received e-mails to personal e-mail account with offers of odd jobs	Possible side job.	Link
20		Employee name	The employee sent and downloaded documents to/from iCloud, which made it clear he had own business.	The employee provides legal services to different companies gaining significantly.	Link
			Ambiguous relationship		
21		Employee name	The employee sent several CVs from personal e-mail accountto to another employee.	Possibly wants to find employment for family.	Link
22		Employee name	Chatting on social network telling about some aquaintance drug addict from Poland who has weapon. Also, telling about her being sexually abused.	Suspicious relations.	Link
23		Employee name	Correspondence on Facebook about intimacy intention meetings.	Suspicious relations.	Link
			Disappointed customers		
24		Employee name	E-mail from a disappointed dissatisfied client in which he complains on the work.	Disappointed client.	Link
			Entrepreneurship and side jobs		
25		Employee name	Too close communication with one client.	Friendly communication with one client who asks to give good prices. Payoffs are possible.	Link
			Miscellaneous		
26		Employee name	Reading reviews on work in the company.		Link
27		Employee name	Watching movies in work time, some days for more than 5 hours.	Misuse of work time and resources.	Link
28		Employee name	In Viber chat wrote that there was a new manager in the company and not clear what to expect.	Discussion of the management.	Link

Rapport bref sur les incidents

AVANTAGES

- Une attitude impartiale et une approche professionnelle - l'équipe d'analystes fournissant nos services ne connaît pas personnellement les employés de l'entreprise, ainsi, le facteur humain est exclu lors des enquêtes.
- Détection des "points faibles" de l'entreprise dans un court laps de temps (les premiers résultats sont généralement obtenus sous 1 mois).
- Profitez de l'expérience et de la base de connaissances d'une entreprise comptant plus de 3 000 clients. Notre équipe sera en mesure d'affiner le système en tenant compte du domaine d'activité de l'entreprise, ainsi que d'utiliser ses fonctionnalités le plus efficacement possible.
- Seuil d'entrée bas : pas besoin de dépenser de l'argent pour l'équipement, la recherche et le salaire d'un spécialiste de la SI, ni perdre le temps pour mettre en œuvre le système. Tout cela est inclus dans l'abonnement mensuel à SI-outsourcing.

Solutions globales SearchInform

SEARCHINFORM ET HUAWEI

La solution mixte SearchInform FileAuditor et Huawei OceanStor offre aux organisations une intégration transparente, permettant toutes les fonctions d'audit de fichiers, y compris la catégorisation, le contrôle d'accès, l'audit des opérations avec les informations confidentielles sur les périphériques SAN OceanStor.

L'utilisation des systèmes de stockage capables de gérer d'énormes quantités de données et de fournir l'accès à un grand nombre d'utilisateurs est indispensable de nos jours. Le problème est que de tels stockages nécessitent un respect irréprochable des règles de sécurité et un haut niveau de protection des données.

Pour stocker les données en toute sécurité et savoir où se trouvent les informations sensibles, qui les utilise ou y apporte des modifications, il est important d'équiper les systèmes d'entreprise d'analyses intelligentes et de surveiller le stockage à l'aide d'un système d'audit de fichiers.

- Classification des données sensibles
- Archivage des documents critiques
- Audit des droits d'accès
- Suivi de l'activité utilisateurs

- L'entreprise obtient une solution unique car SearchInform FileAuditor et Huawei OceanStor s'intègrent de manière transparente.
- Pas besoin de déployer d'autres solutions et d'assurer leurs fonctionnent commun
- Capacités intégrées d'audit des opérations avec les informations et la liste de contrôle d'accès
- Catégorisation automatisée des données stockées en fonction de leur contenu
- Stockage persistant et isolé des clichés instantanés de fichiers sensibles
- Détection des violations des règles de stockage et des abus d'accès

SEARCHINFORM ET MICROSOFT

SearchInform propose un système complet désormais disponible sur Microsoft Azure, une solution cloud fiable qui répond aux normes et aux exigences définies par les entreprises multinationales et les organisations gouvernementales.

Microsoft Azure

Microsoft Azure est soutenu par 3 500 experts en cybersécurité pour fournir aux clients un niveau élevé de protection de l'infrastructure et des flux de travail. Azure se soucie des données d'entreprise car une organisation a un contrôle total sur ses données, le partage à des fins de marketing est interdit. Le marché permet aux fournisseurs de présenter les versions de leurs logiciels adaptées au fonctionnement dans un environnement virtuel.

Collaboration avec Microsoft garantit que les outils de protection des données et de prévention des menaces internes de SearchInform sont disponibles partout dans le monde, car leur présence sur la plate-forme assure la qualité et l'applicabilité dans le cadre des règles et réglementations de Microsoft.

Effectuez les 4 étapes suivantes pour déployer une solution SearchInform sur Microsoft Azure

1. Sélectionnez notre produit dans Azure
2. Choisissez un système de stockage et l'emplacement du SGBD
3. Vérifiez les licences et installez-les dans le centre de données
4. Déployez des logiciels sur des ordinateurs

CONTACTES

ARGENTINE
Buenos Aires
Téléphones : +54 0 11 5984 2618
+54 9 11 5158 8557
Email: r.martinez@searchinform.com

BÉLARUS
Minsk
Téléphone : +375 17 227 56 80
Email: order@searchinform.ru

BRÉSIL
São Paulo
Téléphone : +55 11 9 8973 2037
Email: s.bertoni@searchinform.com

KAZAKHSTAN
Almaty
Téléphones : +7 705 188 98 85
+7 777 239 30 36
Email: d.stelchenko@searchinform.ru

MOYEN-ORIENT ET AFRIQUE
Téléphone : +375 33 344 85 90
Email: yamen@searchinform.com

RUSSIE
Moscou
Téléphones : +7 495 721 84 06
+7 499 703 04 57
Email: info@searchinform.ru

AFRIQUE DU SUD
Centurion
Téléphone : +27 12 683 8816
Email: jorina@searchinform.com

NOS CLIENTS

PROEMISA

weg

NTIYISO CONSULTING

equip

المؤسسة الفلسطينية لضمان الودائع
PALESTINE DEPOSIT INSURANCE CORPORATION

mtl MUANG THAI LIFE