

SEARCHINFORM SOLUTION: INTERNAL THREAT MITIGATION



*Mohamed Salah Sayari
Responsable vente et développement
Commercial en Afrique*



SEARCHINFORM

Actuellement

15+ ans au marché de gestion des risques

25+ ans dans le domaine informatique

3 000+ clients dans **20+** pays

3 000 000+ Ordinateurs
sont protégés par les produits Searchinform

DLP Reconnu par Gartner depuis **2017**

Annuel de Road Shows dans APAC, MENA et CIS





*Une approche comprehensive
à la sécurité de l'information
et à la gestion des risques.*

NIVEAUX DE SÉCURITÉ DES INFORMATIONS

Niveau de base

Solution DCAP pour l'audit automatisé du système de fichiers, la recherche de violations d'accès et la surveillance des modifications des données critiques

File Auditor DCAP

Niveau avancé

Protection des données au niveau des postes de travail, contrôle des canaux de données

DLP

Niveau expert

Nouvelle génération de DLP avec des outils d'investigation. Plate-forme de protection interne

Risk Monitor

Tous les systèmes sont intégrés de manière transparente, fonctionnent sur une plate-forme technologique unique et peuvent être déployés en quelques heures. L'ajout de l'un des systèmes augmente considérablement la fonctionnalité du complexe

Indexing Workstations = e-Discovery

Permet de détecter l'occurrence, la copie, le déplacement et la suppression de données sensibles sur les postes de travail des utilisateurs en temps réel,

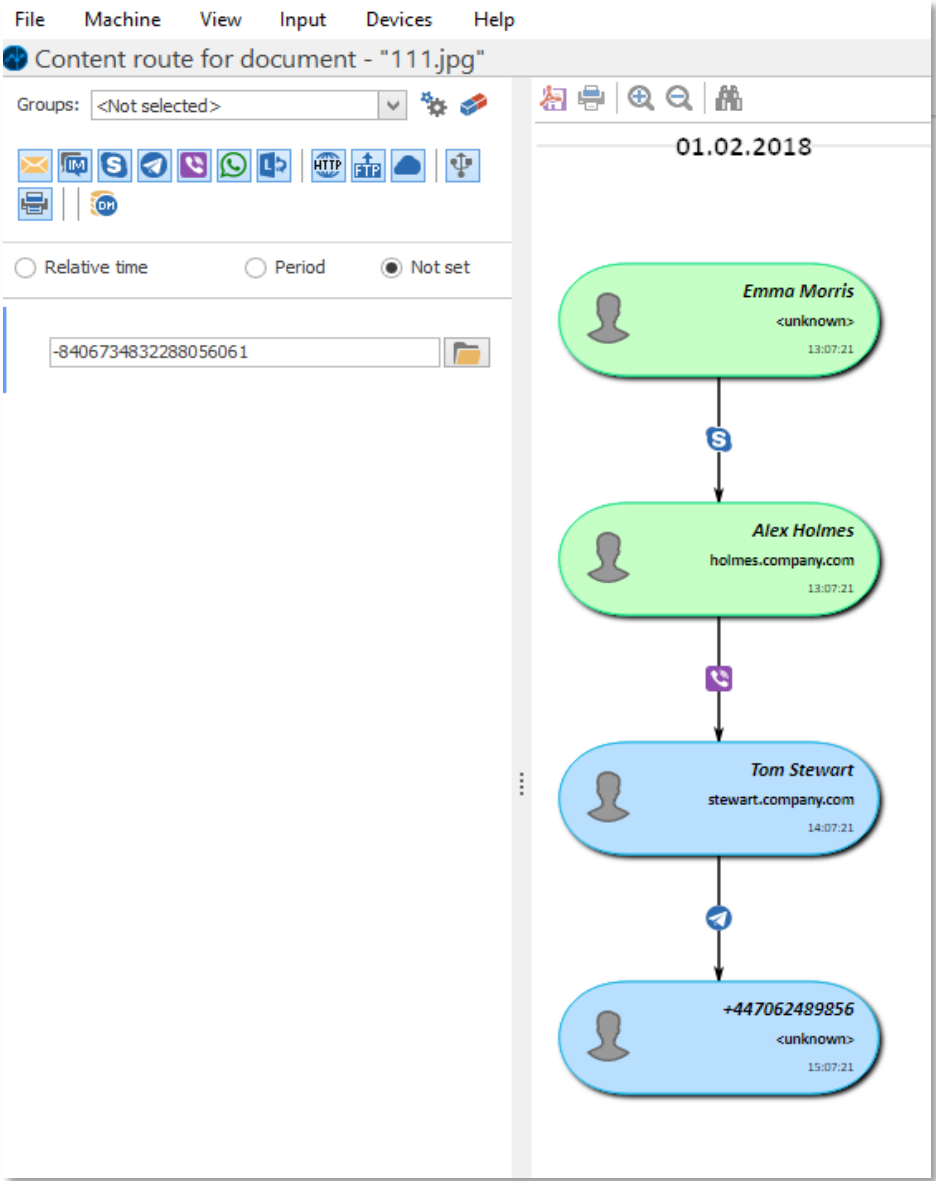
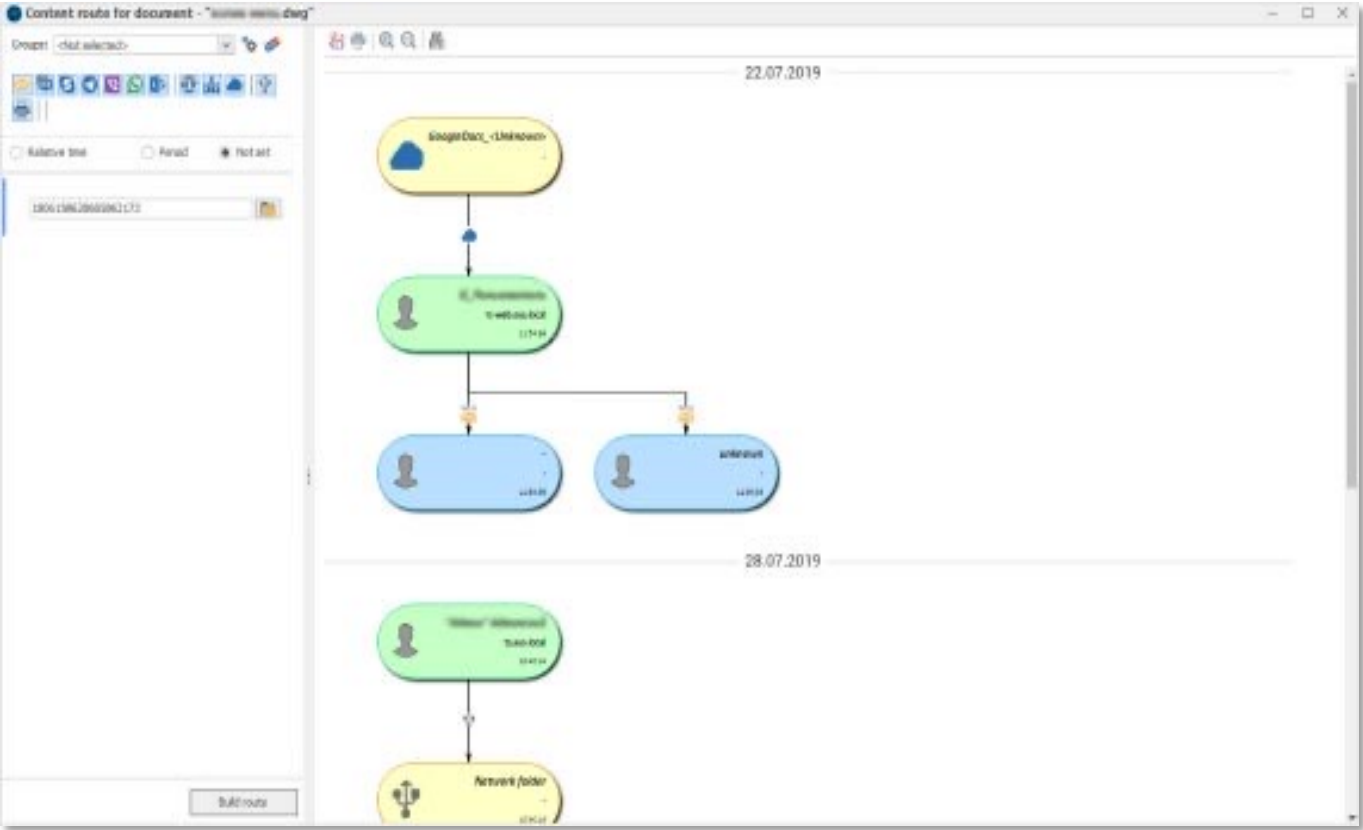
The screenshot displays a Windows search window with a list of files and a preview of a document. The file list includes columns for ID, Date/Time, File Type, Computer, IP, Size, File Name, Path, Date Created, and Date Updated. The preview shows text related to information security concepts.

ID	Дата/Время	Тип файла	Компьютер	IP	Размер	Имя файла	Путь	Дата создания	Дата обновления
1	03.04.2025 21:30:32	Документ	WIN7.ds201.local		13,8 КБ	C:\Users\manager2\Desktop\Открытый код\Структура концепции защиты.docx	C:\Users\manager2\Desktop\Открытый код\	03.04.2025 21:30:32	17.02.2020 8:49:24
3	03.04.2025 21:30:32	Документ	WIN7.ds201.local		13,8 КБ	C:\Users\manager2\Desktop\Открытый код\Структура концепции защиты.docx	C:\Users\manager2\Desktop\Открытый код\	03.04.2025 21:30:32	17.02.2020 8:49:24
4	03.04.2025 21:30:32	Документ	WIN7.ds201.local		73,0 КБ	C:\Users\manager2\Desktop\Открытый код\Политика информационной безопасности.docx	C:\Users\manager2\Desktop\Открытый код\	03.04.2025 21:30:32	17.02.2020 8:55:28
5	03.04.2025 21:30:32	Документ	WIN7.ds201.local		73,0 КБ	C:\Users\manager2\Desktop\Открытый код\Политика информационной безопасности.docx	C:\Users\manager2\Desktop\Открытый код\	03.04.2025 21:30:32	17.02.2020 8:55:28
6	03.04.2025 21:30:32	Документ	WIN7.ds201.local		73,0 КБ	C:\Users\manager2\Desktop\Открытый код\Политика информационной безопасности.docx	C:\Users\manager2\Desktop\Открытый код\	03.04.2025 21:30:32	17.02.2020 8:55:28
7	03.04.2019 16:35:15	Документ	WIN7.ds201.local		306 КБ	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml.msgf1...	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml...	20.03.2019 19:29:59	03.04.2019 16:35:15
8	03.04.2019 16:35:15	Документ	WIN7.ds201.local		306 КБ	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml.msgf1...	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml...	20.03.2019 19:29:59	03.04.2019 16:35:15
9	03.04.2019 16:35:15	Документ	WIN7.ds201.local		306 КБ	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml.msgf1...	C:\Users\manager2\Desktop\Новая папка\1474004909.M595768P49623.sogo.bngf.eml...	20.03.2019 19:29:59	03.04.2019 16:35:15
10	18.10.2017 16:39:55	Документ	WIN7.ds201.local		926 КБ	C:\Users\manager2\Desktop\трест.mxl	C:\Users\manager2\Desktop\	18.10.2017 16:39:55	18.10.2017 16:39:33
11	18.10.2017 16:39:55	Документ	WIN7.ds201.local		926 КБ	C:\Users\manager2\Desktop\трест.mxl	C:\Users\manager2\Desktop\	18.10.2017 16:39:55	18.10.2017 16:39:33
12	18.10.2017 16:39:55	Документ	WIN7.ds201.local		926 КБ	C:\Users\manager2\Desktop\трест.mxl	C:\Users\manager2\Desktop\	18.10.2017 16:39:55	18.10.2017 16:39:33
13	18.10.2017 16:31:09	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Инструкции.rar\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\Инструкции.rar\	18.10.2017 16:31:09	07.10.2014 16:00:18
14	18.10.2017 16:31:09	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Инструкции.rar\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\Инструкции.rar\	18.10.2017 16:31:09	07.10.2014 16:00:18
15	18.10.2017 16:31:09	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Инструкции.rar\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\Инструкции.rar\	18.10.2017 16:31:09	07.10.2014 16:00:18
16	18.10.2017 16:29:15	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\Список кодов ошибок Windo...	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\	18.10.2017 16:29:15	07.10.2014 16:00:18
17	18.10.2017 16:29:15	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\Список кодов ошибок Windo...	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\	18.10.2017 16:29:15	07.10.2014 16:00:18
18	18.10.2017 16:29:15	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\Список кодов ошибок Windo...	C:\Users\manager2\Desktop\Список кодов ошибок Windows.zp\	18.10.2017 16:29:15	07.10.2014 16:00:18
19	18.10.2017 16:14:08	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\	18.10.2017 16:14:08	07.10.2014 15:00:18
20	18.10.2017 16:14:08	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\	18.10.2017 16:14:08	07.10.2014 15:00:18
21	18.10.2017 16:14:08	Документ	WIN7.ds201.local		124 КБ	C:\Users\manager2\Desktop\Список кодов ошибок Windows.doc	C:\Users\manager2\Desktop\	18.10.2017 16:14:08	07.10.2014 15:00:18
22	21.04.2017 11:17:54	Документ	WIN7.ds201.local		15,1 КБ	C:\Очень важные документы\Архивы\Серч КИБ зр.zp\Серч КИБ.docx	C:\Очень важные документы\Архивы\Серч КИБ зр.zp\	03.02.2017 12:42:39	03.02.2017 12:43:22

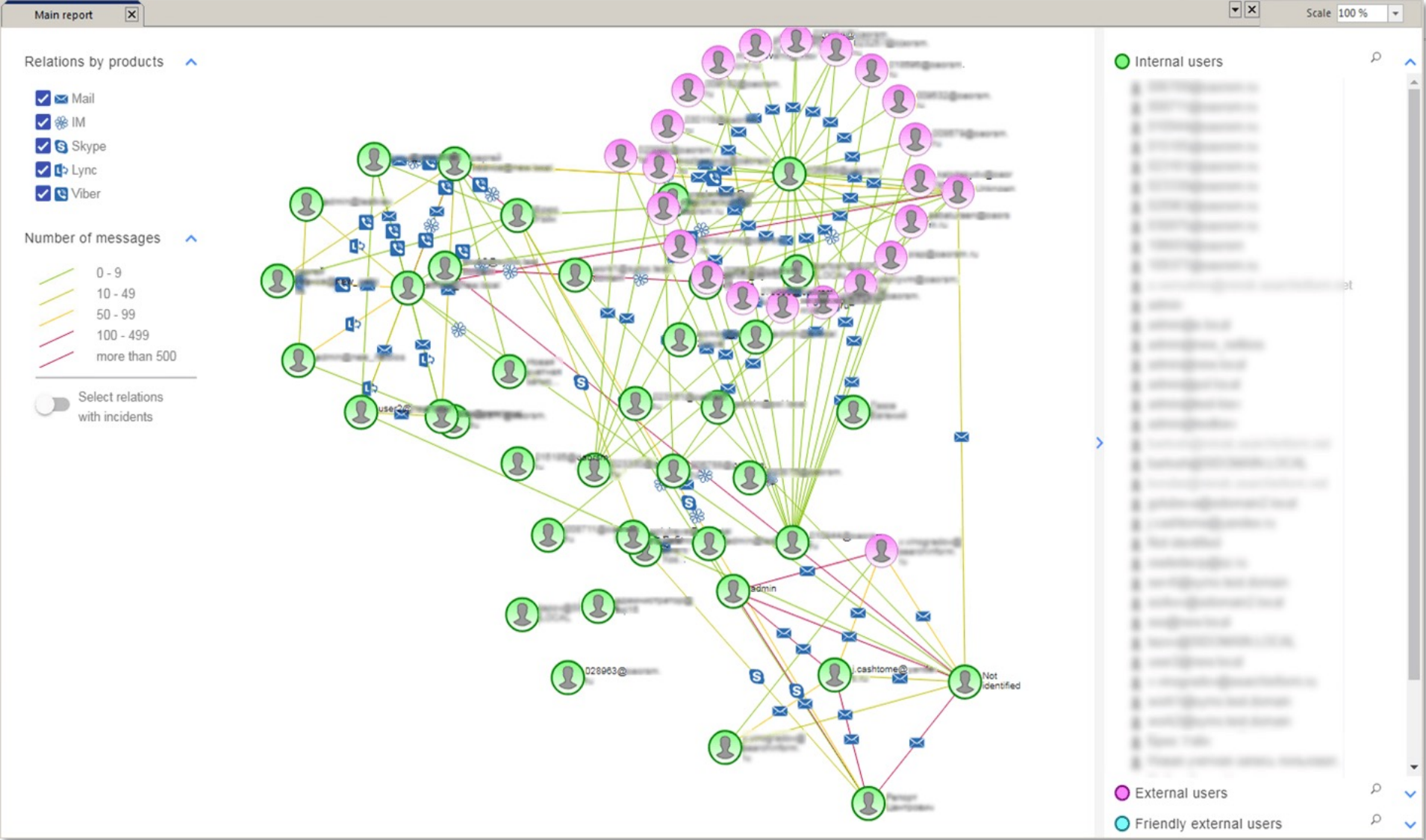
Структура концепции защиты
Сразу заметим: концепция информационной защиты не тождественна стратегии. Первая статична, в то время как вторая - динамична. Основными разделами концепции безопасности являются: определение ИБ; структура безопасности; описание механизма контроля над безопасностью; оценка риска; безопасность информации: принципы и стандарты; обязанности и ответственность каждого отдела, управления или департамента в осуществлении защиты информационных носителей и прочих данных; ссылки на иные нормативы о безопасности. Помимо этого не лишним будет раздел, описывающий основные критерии эффективности в сфере защиты важной информации. Индикаторы эффективности защиты необходимы, прежде всего, топ-менеджменту. Они позволяют объективно оценить организацию безопасности, не углубляясь в технические нюансы. Ответственному за организацию безопасности также необходимо знать четкие критерии оценки эффективности дабы понимать, каким образом руководство будет оценивать его работу.

Активация Windows
Чтобы активировать Windows, перейдите в компонент панели управления "Система".

Analytical instruments : **La Surveillance de l'activité des utilisateurs sur le fichier et le route du contenu du document**



Analytical instruments: *Rapport de communication utilisateur*



DLP

- ✓ Protège l'entreprise contre les fuites d'informations confidentielles
- ✓ Contrôle les données au repos et les données en mouvement.
- ✓ Surveille tous les canaux de transmission de données
- ✓ Analyse les informations, détecte et prévient sur les violations



DLP



Protégez les données en mouvement



Prévention des fuites de données via tous les canaux de transfert de données

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT



**PRÉVENTION DES
FUITES DE
DONNÉES**



**PROTECTION DES
DONNÉES
GRAPHIQUES**



**ARCHIVAGE
DES
DONNÉES**



**CRYPTAGE DES
DONNÉES**



**CENTRE
D'ALERTE**



**INTERCEPTION
IM**



**PROTECTION DU
TRANSFERT DE
DONNÉES
VERS/DEPUIS LES
SERVICES CLOUD**



**PROTECTION DES
FILIGRANES SUR
LES CAPTURES
D'ÉCRAN**



**BLOCAGE DES PROCESSUS
ET DES ACTIVITÉS BASÉ
SUR LE CONTENU**

RISK MONITOR

**Neutralise le facteur humain
et protège une entreprise de
tous types de fraudes et
d'incidents internes**



Risk Monitor *Architecture*

NetworkController

Contrôle le trafic au niveau du réseau

- *Reflète le trafic au niveau du réseau de l'entreprise (Switch)*
- *Mail, Messageries instantanée , HTTP, FTP, Cloud.*

EndpointController

Contrôle le trafic au niveau du poste de travail

- *Capture l'activité des employés au moyen d'agents-programmes installés sur les postes de travail ;*
- *Mail, IM, Skype, Device, FTP, Print, HTTP, Files, Monitor, Microphone, Cloud*

Interception Email Traffic: Mail Controller

Capture tous les e-mails entrants et sortants envoyés via des navigateurs Web (Gmail, Yahoo, Hotmail) ou les mails clients (Outlook, etc.)

No.	Category	Type	Date/Time	Attachments	Extensi	Subject	From	To	Domain	Computer	User	From IP	MAC	Size	Participants	Creation date
Type: HTTP (30)																
1	Mail	WEB	2/21/2018 5:55:28...			Information	ohlalmarketing...	Paul Young (p...	company	young.company.com	young@company	10.0.1.24	00-50-56-83-22-BD	607 bytes	1	2/21/2018
2	Mail	WEB	2/21/2018 6:13:44...	1		RE: Information	Paul Young (pa...	ohlalmarketin...	company	young.company.com	young@company	10.0.1.24	00-50-56-83-22-BD	15.1 KB	1	2/21/2018
3	Mail	WEB	2/22/2018 12:30:3...			RE: RE: Information	ohlalmarketing...	Paul Young (p...	company	young.company.com	young@company	10.0.1.24	00-50-56-83-22-BD	896 bytes	1	2/22/2018
4	Mail	WEB	2/22/2018 12:38:5...			RE: RE: RE: Inform...	Paul Young (pa...	ohlalmarketin...	company	young.company.com	young@company	10.0.1.24	00-50-56-83-22-BD	1.16 KB	1	2/22/2018
5	Mail	WEB	8/23/2019 3:37:46...			Apple Push Notifica...	appleid@id.appl...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	5.98 KB	1	7/12/2018
6	Mail	WEB	8/23/2019 3:37:46...			New product. New ...	visualanalysis@...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	34.8 KB	1	4/27/2018
7	Mail	WEB	8/23/2019 3:37:46...			Apple Push Notifica...	appleid@id.appl...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	5.98 KB	1	7/12/2018
8	Mail	WEB	8/23/2019 3:37:46...			Want to extend yo...	sas.viyaep@sa...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	15.2 KB	1	11/24/2018
9	Mail	WEB	8/23/2019 3:37:47...			Get started with Po...	powerbi@micro...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	31.4 KB	1	11/14/2018
10	Mail	WEB	8/23/2019 3:37:46...			Please activate yo...	replies-disabled...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	3.34 KB	1	11/15/2018
11	Mail	WEB	8/23/2019 3:37:46...			Get Started with T...	visualanalysis@...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	35.7 KB	1	12/21/2018
12	Mail	WEB	8/23/2019 3:39:28...			Microsoft Develop...	noreply@youtu...	fileserv@com...	computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	57.7 KB	1	2/17/2018
13	Mail	WEB	8/23/2019 3:39:42...			unknown	fileserv@compu...		computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	739 bytes	0	8/23/2019
14	Mail	WEB	8/23/2019 3:39:44...				fileserv@compu...		computer	computer	fileserv@computer	192.168.50.132	00-0C-29-5A-9A-76	250 bytes	0	8/23/2019

Page: 1 / 1

From: ohlalmarketing@gmail.com
To: <paultheyoungest@gmail.com>
Subject: Information

0 of 0

Hello Paul,

To continue our conversation, I want to reply positively that we are interested in obtaining such information. But firstly we'd like to see an example of pulled data.

Native | Text only | Attributes

Interception des protocoles suivants :

Mail Controller

The screenshot shows the Mail Controller interface. At the top, there are tabs for 'Incidents' and 'Security policy settings'. Below this, there's a section for 'Search criterion parameters' with options like 'New search criterion', 'Edit search criterion', 'Delete criterion', and 'Paste search criterion'. A table lists search criteria: 'Attachment' and 'Personal data', both with 'Attribute search' as the search type. Below the table, there are sections for 'Items to check' (containing 'MailController*') and 'Notification recipients' (showing '<No data to display>'). There's also a 'Schedule of checking' section with a 'Quarantine activity schedule' and a 'Work calendar' button. At the bottom, there are 'Used lists of exceptions' with buttons for 'Add white list', 'Add black list', and 'Remove from list'.

Blockage du Trafic SMTP/IMAP .

The screenshot shows the 'Mail' configuration window. It has a 'Combine using:' dropdown set to 'OR'. There are several checkboxes: 'Exclude attachments' (unchecked), 'Protocols' (checked), 'Excluding' (unchecked), 'Email type' (unchecked), 'From' (unchecked), 'To' (unchecked), and 'Show all' (unchecked). A dropdown menu is open, showing a list of protocols: 'SMTP, POP3, IMAP, HTTP, MAPI, NNTP'. 'SMTP' is selected and highlighted in blue. Other protocols listed are 'POP3', 'IMAP', 'HTTP', 'MAPI', and 'NNTP', all with checked boxes. At the bottom, there are buttons for 'Search in the results' (unchecked), 'Clear', and 'Search'.

Web Mail: *Gmail.com, Outlook.com, Office 365, Yahoo.com, Google Sync. etc.*

Interception data transfer traffic: *FTP Controller*

Capture les données envoyées ou reçues via FTP ,via une connexion ordinaire ou une connexion SSL cryptée.

The screenshot displays the 'Search - Analytic Console' interface. The main area shows a table of search results for FTP traffic. The table has columns for No., Category, Type, Date/Time, Extension, User, Size, File name, FTP server, and FTP login. The results show multiple entries for FTP traffic on 07.03.2017 at 10:05:19, with various file sizes and names. The interface also includes a search filter panel on the left with options for interception date, user, phrase search, similar-content search, search with dictionary, phone number search, search by form, common attributes, and FTP-specific attributes. The bottom of the interface shows the number of documents (605) and the selection time (11 sec).

No.	Category	Type	Date/Time	Extension	User	Size	File name	FTP server	FTP login
1	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	2,39 M6	\\Engineer\771389\2017030...	10.0.2.52	Administrator
2	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	162 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
3	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	153 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
4	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	176 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
5	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	135 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
6	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	169 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
7	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	228 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
8	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	147 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
9	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	366 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
10	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	97,5 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
11	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	173 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
12	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	139 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
13	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	131 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
14	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	131 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
15	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	131 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
16	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	155 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator
17	FTP	FTP	07.03.2017 10:05:19		Administrator@searchinf...	137 KB	\\Engineer\771389\2017030...	10.0.2.52	Administrator

Interception browser traffic: *HTTP Controller*

Search - Analytic Console

Search 3 x +

Groups: <Not selected>

Filter by types: All results

Table view

No.	Category	Date/Time	Attachments	Extension	To	User
1	HTTP	11.01.2019 10:32:27			www.youtube...	User (user@writers.local)
2	HTTP	11.01.2019 10:32:52			www.youtube...	User (user@writers.local)
3	HTTP	11.01.2019 10:33:10			www.youtube...	User (user@writers.local)
4	HTTP	11.01.2019 11:03:24			www.youtube...	User (user@writers.local)
5	HTTP	11.01.2019 11:03:38			www.youtube...	User (user@writers.local)
6	HTTP	11.01.2019 11:04:10			www.youtube...	User (user@writers.local)
7	HTTP	11.01.2019 11:34:03			www.youtube...	User (user@writers.local)
8	HTTP	11.01.2019 11:34:28			www.youtube...	User (user@writers.local)
9	HTTP	11.01.2019 11:34:55			www.youtube...	User (user@writers.local)
10	HTTP	11.01.2019 12:15:05			www.youtube...	User (user@writers.local)
11	HTTP	11.01.2019 12:15:13			www.youtube...	User (user@writers.local)
12	HTTP	11.01.2019 12:15:24			www.youtube...	User (user@writers.local)
13	HTTP	11.01.2019 12:27:19			autoupdate.g...	User (user@writers.local)
14	HTTP	11.01.2019 12:45:58			www.youtube...	User (user@writers.local)
15	HTTP	11.01.2019 12:46:13			www.youtube...	User (user@writers.local)
16	HTTP	11.01.2019 12:46:29			www.youtube...	User (user@writers.local)
17	HTTP	11.01.2019 13:16:39			www.youtube...	User (user@writers.local)

Page: 1 / 3

Word wrap

0 of 0

URL=www.youtube.com/ad_data_204

```
dt=1545816424632
flash=0
frm=2
u_tz=180
u_his=9
u_java=false
u_h=927
u_w=1597
u_ah=887
u_aw=1597
**_nd=74
```

Native Text only Attributes

Number of documents sh 1000 (2575)

Capture les fichiers et les messages envoyés via HTTP(s) et vous permet de contrôler :

- *Forums Internet*
- *Feedback forms;*
- *Web-based IM clients;*
- *Blogs;*
- *Chats Web ;*
- *Réseau Sociaux .*

Interception Chat Apps: IM Controller

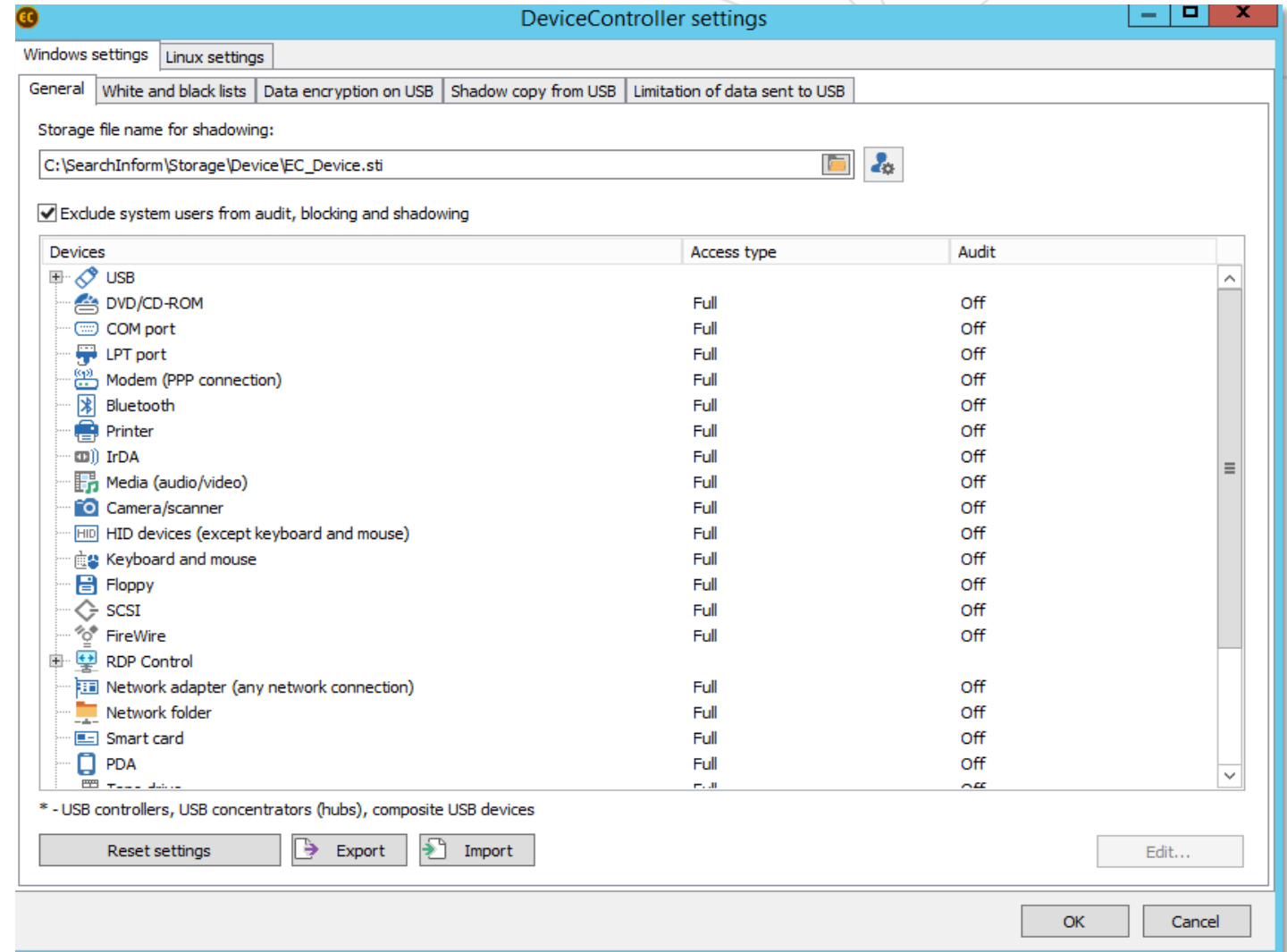
Capture les chats sur les réseaux sociaux (*LinkedIn, Facebook, WhatsApp, Telegram* etc.) et messageries instantanées (*MSN, Jabber, ICQ* etc), ainsi que les messages entrants et sortants d'autres sites populaires.

The screenshot displays the IM Controller interface. On the left, there are filter options for interception date, user, phrase search, similar-content search, search with dictionary, phone number search, and search by form. Below these are sections for Common, Telegram, and IM filters. The main area shows a table of intercepted messages with columns for Type, No., Date/Time, Attachments, Extensi, Subject, From, To, From UIN, To UIN, Domain, Computer, User, From IP, To IP, MAC, and Size. The table is filtered by 'All results' and shows messages from WhatsApp, Viber, and Telegram. Below the table, there is a chat view showing a conversation between WhatsApp_+447040303701 and Harry Smith (WhatsApp_+447047353711). The chat messages are:

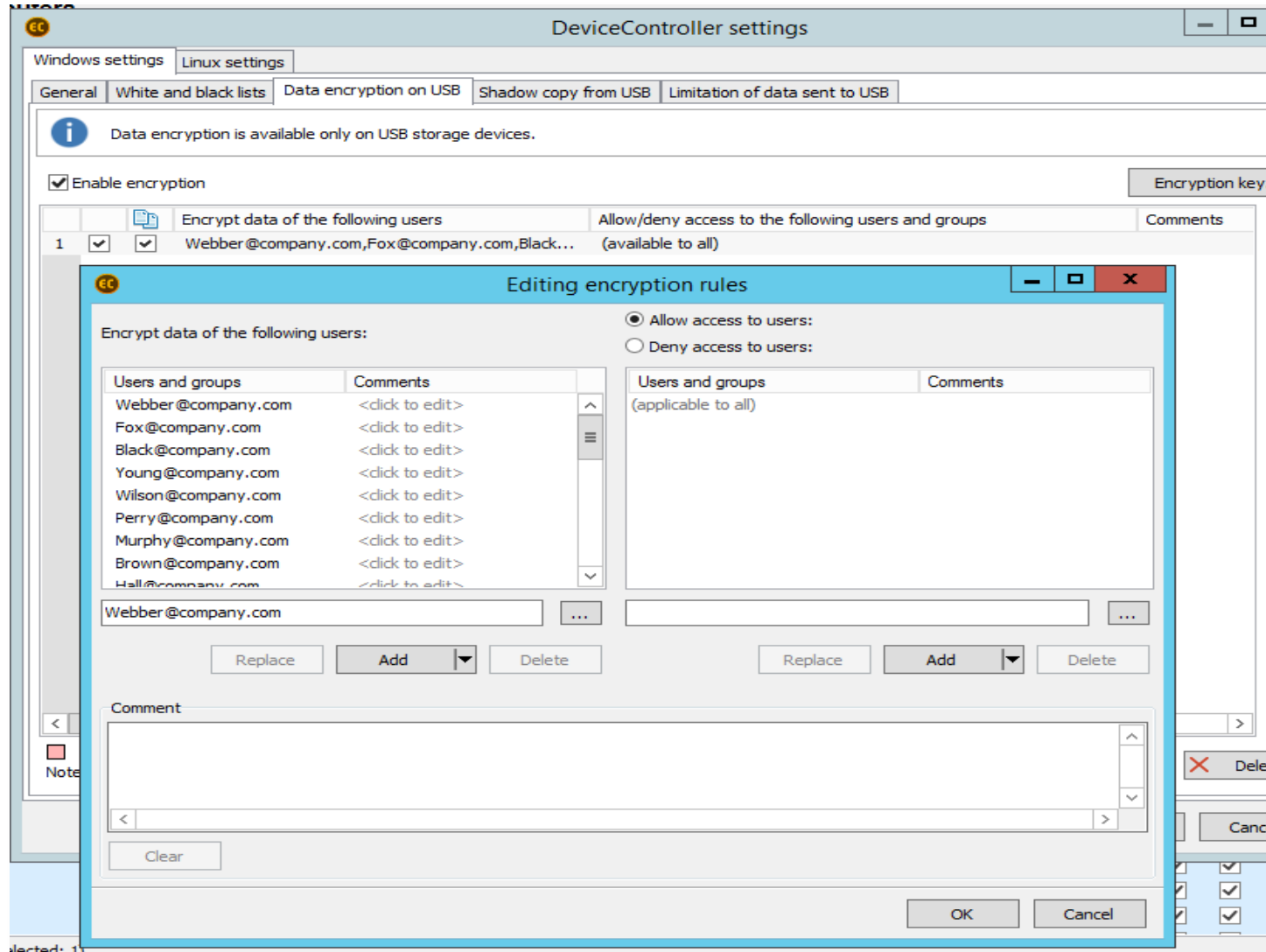
- WhatsApp_+447040303701 (WhatsApp_+447040303701) 10:07:21 05.02.2018: sup man, how s the family
- Harry Smith (WhatsApp_+447047353711) 10:08:10 05.02.2018: not much man, work as usual. Family's all good, whats up with you?
- WhatsApp_+447040303701 (WhatsApp_+447040303701) 10:09:21 05.02.2018: good to hear bro. Can you do me a favor?
- Harry Smith (WhatsApp_+447047353711) 10:10:15 05.02.2018: (no text visible)

Device Controller

- Capture et bloque les données transférées vers les clés USB, les disques durs externes, les CD/DVD et les appareils photo. Crypte automatiquement les données écrites sur un lecteur flash. Il détecte et reconnaît les smartphones connectés à un PC (Android, Apple, BlackBerry, Windows Phone), analyse leur contenu lorsqu'il est connecté en mode drive. Il contrôle l'accès de périphérique à un PC.*



Device Controller: *Special Features*



- *Audit + Blocage d'accès ;*
- *Seulement Blocage d'accès;*
- *Audit + Blocage d'accès+ Shadow Copy;*
- *Blocage total*

Interception data transfer traffic: *Cloud Controller*

Monitorer le trafic entrant ou sortant sur Cloud

- Google Drive;
- Just Cloud;
- Mega;
- OneDrive;
- Evernote;
- Dropbox.

The screenshot displays the 'Search - Analytic Console' interface. The main area shows search results for 'Search 2' with a table of intercepted traffic. The table columns are: No., Date/Time, Extens, From, Domain, Computer, User, From IP, To IP, MAC, and Size. The results show traffic from various domains like 'company.local' and 'ro.local' to 'ro.local' and 'company.local'.

No.	Date/Time	Extens	From	Domain	Computer	User	From IP	To IP	MAC	Size
1	10/21/2014 3:18:5...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	94.0 KB
2	10/21/2014 3:18:5...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	9.00 KB
3	10/21/2014 3:20:1...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	758 KB
4	10/21/2014 3:20:3...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	33.6 KB
5	10/21/2014 3:21:2...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	461 KB
6	10/21/2014 3:21:5...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	126 KB
7	10/21/2014 3:22:1...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	109 KB
8	10/21/2014 3:22:2...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	11.2 KB
9	10/21/2014 3:22:2...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	8.50 KB
10	10/21/2014 3:22:3...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	46.0 KB
11	10/21/2014 3:24:0...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	589 KB
12	10/21/2014 3:24:2...	DropBox_dhwal...	DropBox_dhwal...	company.local	Rogers.company.local	Rogers@company.local	192.168.100.126	184.73.250.168	00-50-56-87-52-70	98.2 KB
13	10/22/2014 2:58:4...	SharePoint_Link...	SharePoint_Link...	ro.local	calli.ro.local	user4@ro.local	10.0.12.66	87.245.216.27	00-50-56-87-5F-33	7.72 KB
14	10/22/2014 2:58:4...	SharePoint_Link...	SharePoint_Link...	ro.local	calli.ro.local	user4@ro.local	10.0.12.66	87.245.216.27	00-50-56-87-5F-33	8.44 KB
15	10/22/2014 2:58:4...	SharePoint_Link...	SharePoint_Link...	ro.local	calli.ro.local	user4@ro.local	10.0.12.66	87.245.216.27	00-50-56-87-5F-33	1.07 KB
16	10/22/2014 2:58:4...	SharePoint_Link...	SharePoint_Link...	ro.local	calli.ro.local	user4@ro.local	10.0.12.66	87.245.216.27	00-50-56-87-5F-33	2.48 KB
17	10/22/2014 2:58:4...	SharePoint_Link...	SharePoint_Link...	ro.local	calli.ro.local	user4@ro.local	10.0.12.66	87.245.216.27	00-50-56-87-5F-33	89.0 KB

Below the table, there is a preview of a spreadsheet with columns A through O and rows 1 through 11. The spreadsheet contains a table with columns: Date, Log In, Log Out, Total Hours, Total Pay. The data rows are: Monday (10:00 AM, 2:00 PM, 4:00, \$40.00), Tuesday (0:00, 0:00, \$0.00), Wednesday (0:00, 0:00, \$0.00), Thursday (0:00, 0:00, \$0.00).

Print Controller

- Surveille le contenu des documents envoyés aux imprimantes quel que soit le modèle d'imprimante, car la capture a lieu au niveau du système d'exploitation

The screenshot displays the Search Inform interface with a search result for a document. The document content is as follows:

ALPHA&CO LTD.
End-year bonuses for the management

Confidential!!!
Approved by: James Black
Approval date: 15 January 2018

James Black	+600,000
Stanley Mayer	+280,000
Diana Connor	+200,000
Harry Smith	+130,000
Henry Brooks	+120,000
Christopher Turner	+120,000
Scott Mitchell	+115,000
Antonie Wilson	+100,000

The interface also shows a table of search results at the top:

# No.	Date/Time	Subject	Printer name	Domain	Computer	User	From IP	MAC	Size	Number of p	Number of o
1	2/1/2018 11:41:39...	Microsoft Word - B...	Printer Of...	company.com	mayer.company.com	Stanley Mayer (mayer@co...	10.0.2.46	00-50-56-83-2E-F0	353 bytes	1	1
2	2/1/2018 11:43:51...	Microsoft Word - B...	Printer Of...	company.com	mayer.company.com	Stanley Mayer (mayer@co...	10.0.2.46	00-50-56-83-2E-F0	353 bytes	1	1

TIME INFORMER : Program Controller

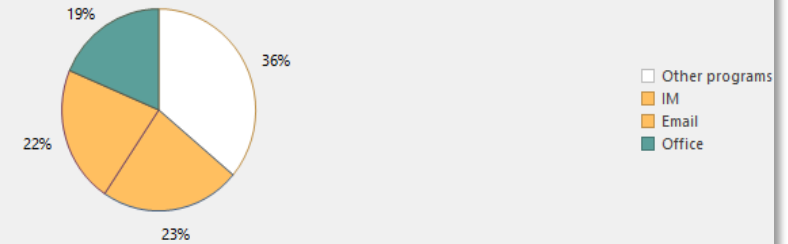
port on user relations × Total duration of working day users × Total active time of processes users by groups × Total time of activity of processes/sites users by groups × Detailed information on users ×

Detailed information on users(period not set)

Information on users

User	Days	Activity	Active (avg.)	Inactive	Inactive (avg.)	Early arrivals	Late departures	Late arrivals	Early departures				
Alex Holmes	20	112:05	5:36	65:08	3:15	0	4	8	4	0	19	0	0
Andrew Spencer	20	128:30	6:25	48:55	2:26	20	0	0	20	0	0	0	0
Antonie Wilson	20	113:59	5:41	69:48	3:29	11	0	2	4	0	0	0	0
Barbara Davis	20	109:39	5:28	74:06	3:42	12	0	0	4	0	0	0	0
Christine Parker	20	111:50	5:35	67:26	3:22	4	2	5	1	0	0	0	0
Christopher Turner	20	111:51	5:35	70:10	3:30	4	4	1	1	0	0	0	0
Daniel Murphy	20	109:30	5:28	67:57	3:23	4	0	4	9	0	4	0	0
David Brown	20	120:55	6:02	59:00	2:57	20	0	0	20	0	0	0	0
Diana Connor	20	130:48	6:32	55:40	2:47	11	4	1	2	0	0	0	0
Emma Morris	20	122:28	6:07	55:20	2:46	20	0	0	20	0	0	0	0
Harry Smith	20	117:17	5:51	69:21	3:28	12	4	0	4	0	15	0	1
Henry Brooks	20	115:00	5:45	68:40	3:26	12	0	0	3	0	0	0	0
Jack Perry	20	114:15	5:42	70:20	3:31	6	0	0	0	0	0	0	0

Running applications Open sites Running applications/active sites

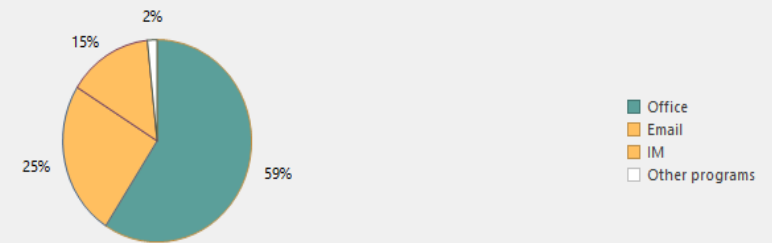


Detailed information on users(period not set)

Information on users

User	Days	Activity	Active (avg.)	Inactive	Inactive (avg.)	Early arrivals	Late departures	Late arrivals	Early departures				
Alex Holmes	20	112:05	5:36	65:08	3:15	0	4	8	4	0	19	0	0
Andrew Spencer	20	128:30	6:25	48:55	2:26	20	0	0	20	0	0	0	0
Antonie Wilson	20	113:59	5:41	69:48	3:29	11	0	2	4	0	0	0	0
Barbara Davis	20	109:39	5:28	74:06	3:42	12	0	0	4	0	0	0	0
Christine Parker	20	111:50	5:35	67:26	3:22	4	2	5	1	0	0	0	0
Christopher Turner	20	111:51	5:35	70:10	3:30	4	4	1	1	0	0	0	0
Daniel Murphy	20	109:30	5:28	67:57	3:23	4	0	4	9	0	4	0	0
David Brown	20	120:55	6:02	59:00	2:57	20	0	0	20	0	0	0	0
Diana Connor	20	130:48	6:32	55:40	2:47	11	4	1	2	0	0	0	0
Emma Morris	20	122:28	6:07	55:20	2:46	20	0	0	20	0	0	0	0
Harry Smith	20	117:17	5:51	69:21	3:28	12	4	0	4	0	15	0	1
Henry Brooks	20	115:00	5:45	68:40	3:26	12	0	0	3	0	0	0	0
Jack Perry	20	114:15	5:42	70:20	3:31	6	0	0	0	0	0	0	0

Running applications Open sites Running applications/active sites



TIME INFORMER : Program Controller

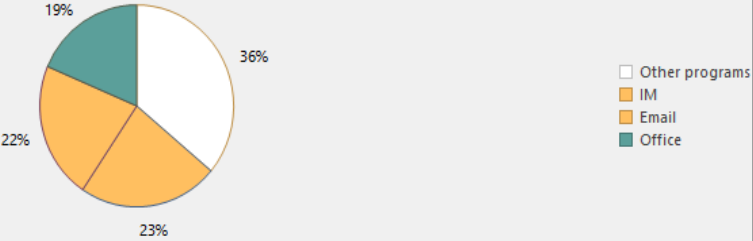
port on user relations × Total duration of working day users × Total active time of processes users by groups × Total time of activity of processes/sites users by groups × Detailed information on users ×

Detailed information on users(period not set)

Information on users

User	Days	Activity	Active (avg.)	Inactive	Inactive (avg.)	Early arrivals	Late departures	Late arrivals	Early departures	IM	Email	Office	Other programs
Alex Holmes	20	112:05	5:36	65:08	3:15	0	4	8	4	0	19	0	0
Andrew Spencer	20	128:30	6:25	48:55	2:26	20	0	0	20	0	0	0	0
Antonie Wilson	20	113:59	5:41	69:48	3:29	11	0	2	4	0	0	0	0
Barbara Davis	20	109:39	5:28	74:06	3:42	12	0	0	4	0	0	0	0
Christine Parker	20	111:50	5:35	67:26	3:22	4	2	5	1	0	0	0	0
Christopher Turner	20	111:51	5:35	70:10	3:30	4	4	1	1	0	0	0	0
Daniel Murphy	20	109:30	5:28	67:57	3:23	4	0	4	9	0	4	0	0
David Brown	20	120:55	6:02	59:00	2:57	20	0	0	20	0	0	0	0
Diana Connor	20	130:48	6:32	55:40	2:47	11	4	1	2	0	0	0	0
Emma Morris	20	122:28	6:07	55:20	2:46	20	0	0	20	0	0	0	0
Harry Smith	20	117:17	5:51	69:21	3:28	12	4	0	4	0	15	0	1
Henry Brooks	20	115:00	5:45	68:40	3:26	12	0	0	3	0	0	0	0
Jack Perry	20	114:15	5:42	70:20	3:31	6	0	0	0	0	0	0	0

Running applications Open sites Running applications/active sites

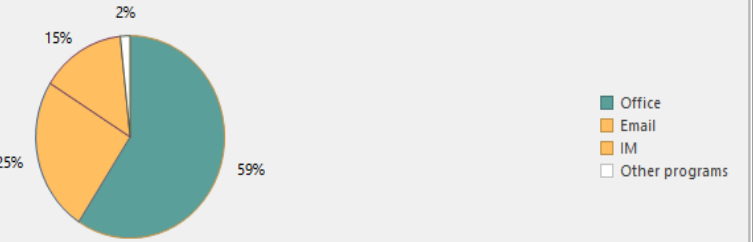


Detailed information on users(period not set)

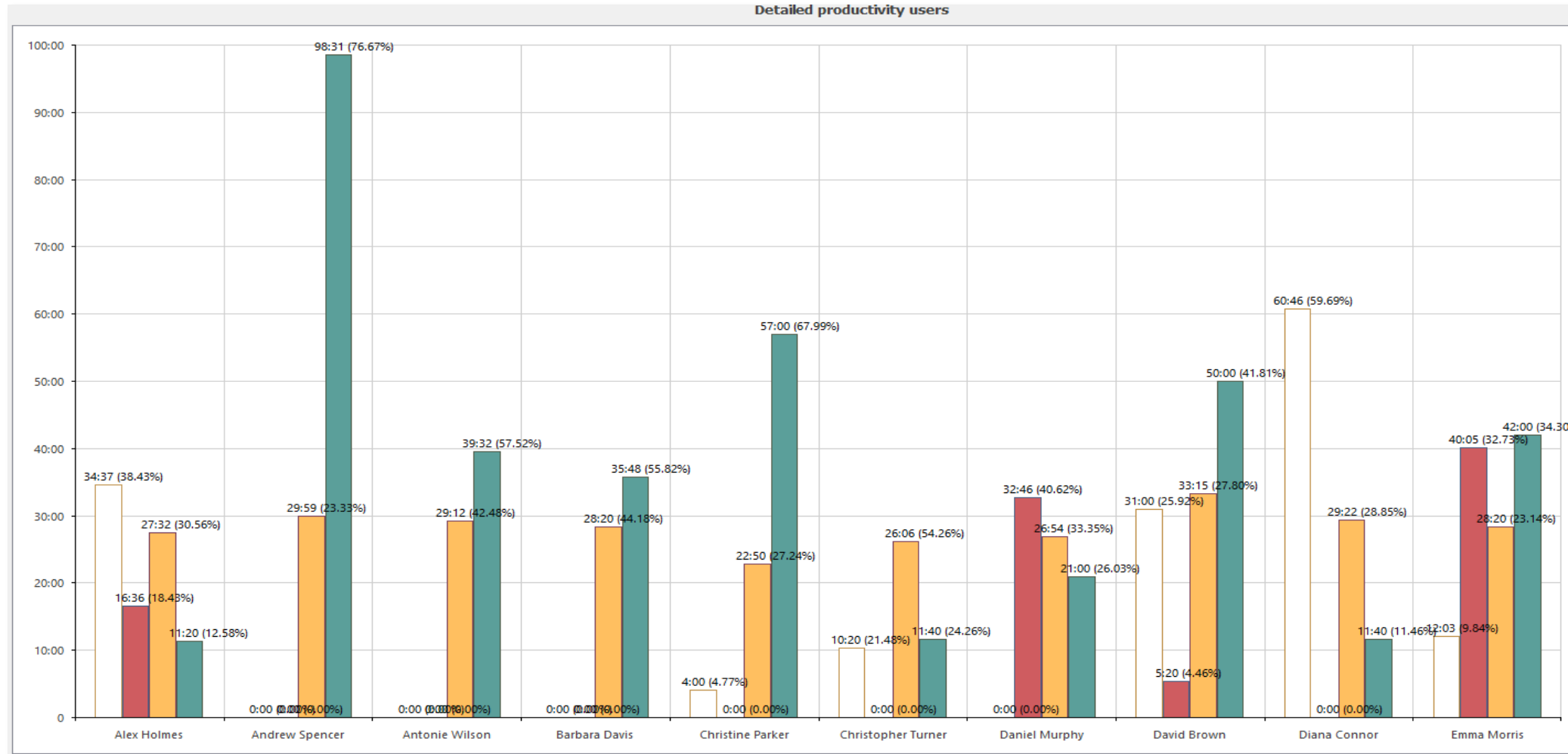
Information on users

User	Days	Activity	Active (avg.)	Inactive	Inactive (avg.)	Early arrivals	Late departures	Late arrivals	Early departures	IM	Email	Office	Other programs
Alex Holmes	20	112:05	5:36	65:08	3:15	0	4	8	4	0	19	0	0
Andrew Spencer	20	128:30	6:25	48:55	2:26	20	0	0	20	0	0	0	0
Antonie Wilson	20	113:59	5:41	69:48	3:29	11	0	2	4	0	0	0	0
Barbara Davis	20	109:39	5:28	74:06	3:42	12	0	0	4	0	0	0	0
Christine Parker	20	111:50	5:35	67:26	3:22	4	2	5	1	0	0	0	0
Christopher Turner	20	111:51	5:35	70:10	3:30	4	4	1	1	0	0	0	0
Daniel Murphy	20	109:30	5:28	67:57	3:23	4	0	4	9	0	4	0	0
David Brown	20	120:55	6:02	59:00	2:57	20	0	0	20	0	0	0	0
Diana Connor	20	130:48	6:32	55:40	2:47	11	4	1	2	0	0	0	0
Emma Morris	20	122:28	6:07	55:20	2:46	20	0	0	20	0	0	0	0
Harry Smith	20	117:17	5:51	69:21	3:28	12	4	0	4	0	15	0	1
Henry Brooks	20	115:00	5:45	68:40	3:26	12	0	0	3	0	0	0	0
Jack Perry	20	114:15	5:42	70:20	3:31	6	0	0	0	0	0	0	0

Running applications Open sites Running applications/active sites

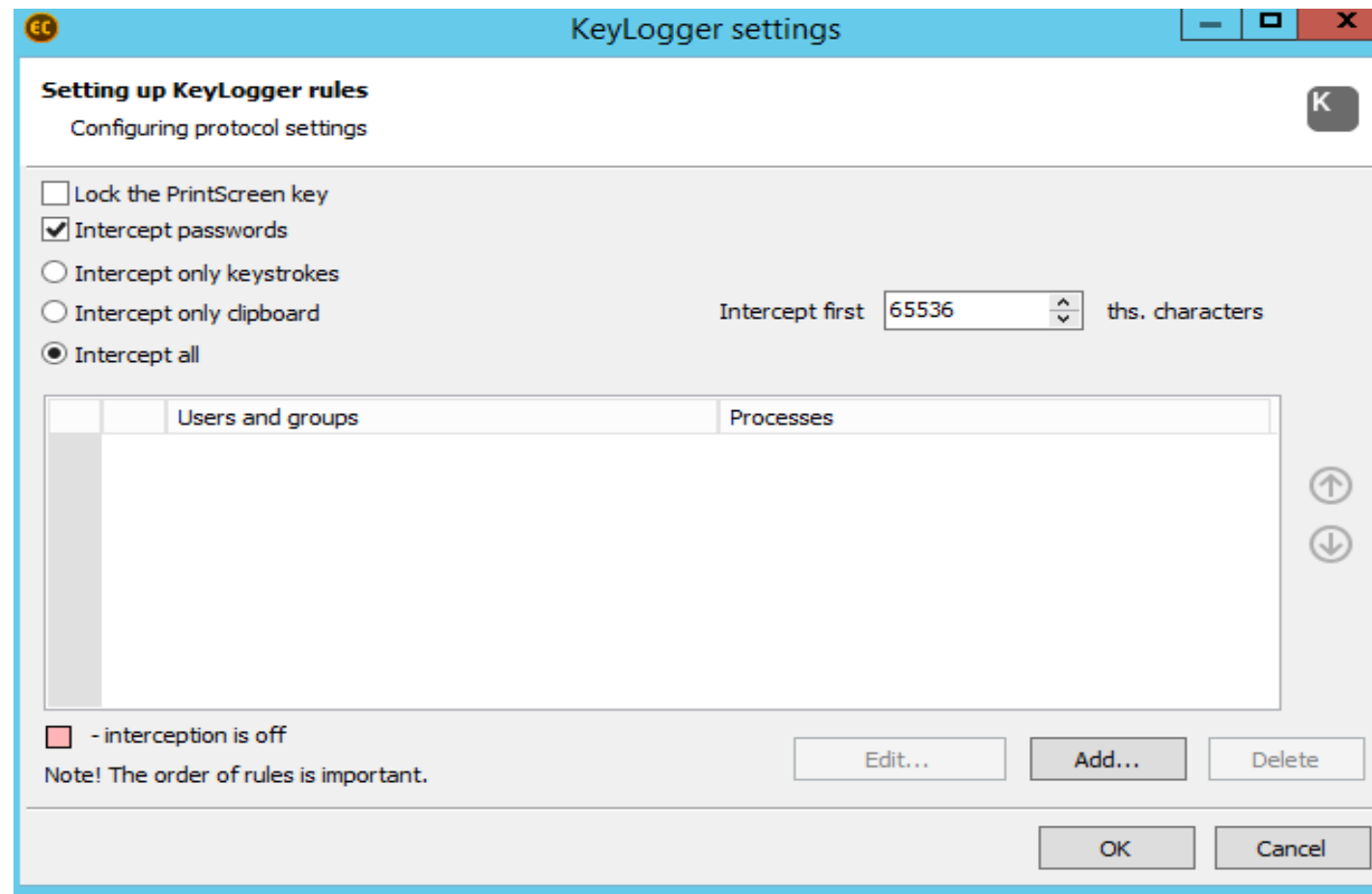


TIME INFORMER : Program Controller



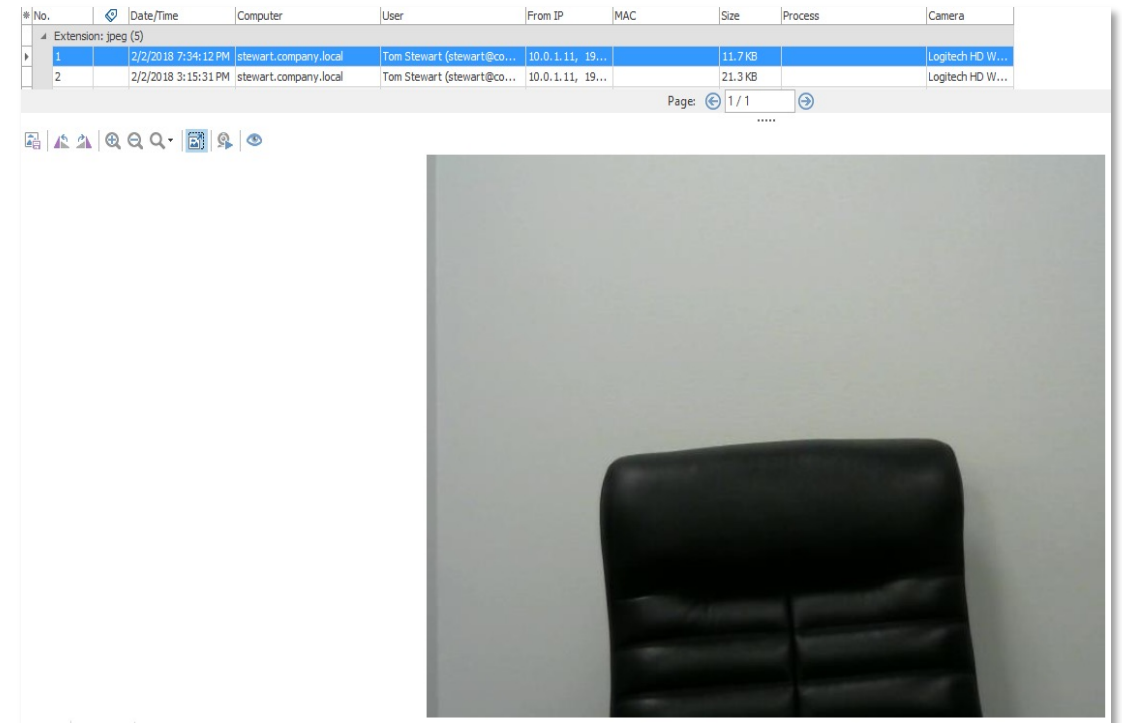
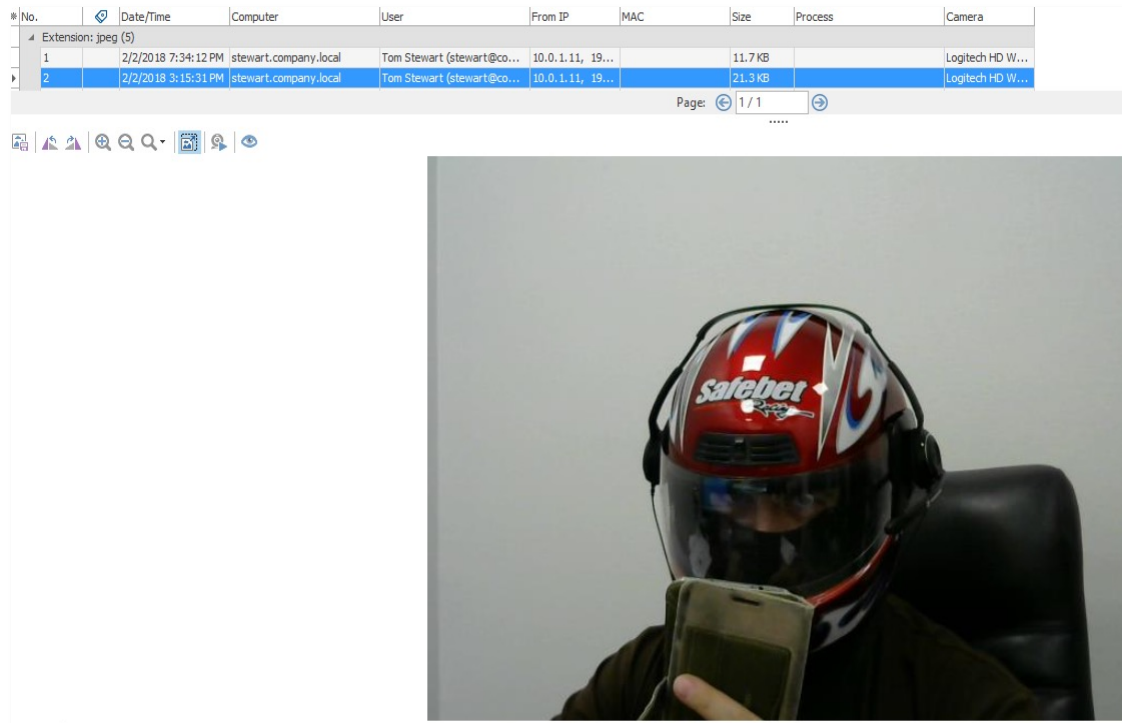
Keylogger

Capture les frappes au clavier (logins, mots de passe, etc.) ainsi que les données copiées dans le presse-papiers. Vous permet de suivre les informations d'identification utilisées pour accéder à des ressources potentiellement dangereuses.



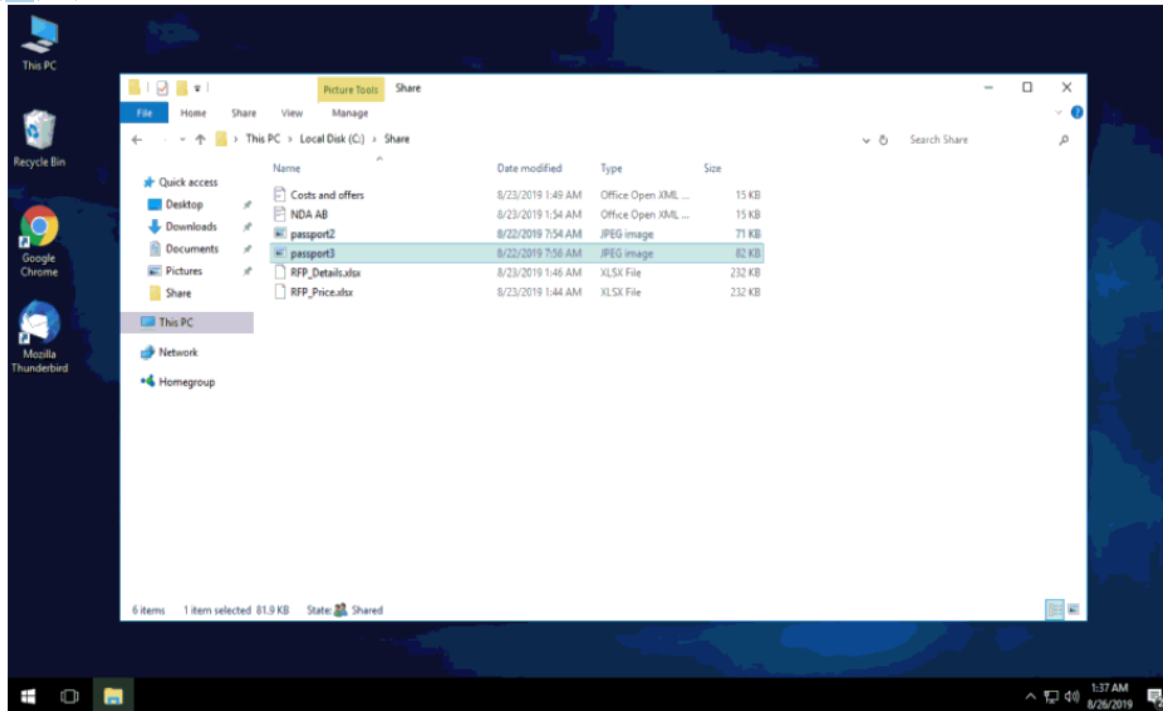
Camera Controller

Prendre une photo ou enregistrer une vidéo de la personne utilisant l'ordinateur



Monitor Controller

*No.	Date/Time	Extensi	Computer	User	From IP	MAC	Size	Process/URL	Screen num	Reason
1	8/26/2019 1:37:31...		computer	fileserv@computer	192.168.50.138	00:0C:29:5A:9A:76	38.4 KB	explorer.exe	1	Timeout
2	8/26/2019 1:37:28...		computer	fileserv@computer	192.168.50.138	00:0C:29:5A:9A:76	37.9 KB	explorer.exe	1	Window c...
3	8/23/2019 4:05:08...		computer	fileserv@computer	192.168.50.132	00:0C:29:5A:9A:76	170 KB	explorer.exe	1	Timeout
4	8/23/2019 4:03:49...		computer	fileserv@computer	192.168.50.132	00:0C:29:5A:9A:76	84.2 KB	explorer.exe	1	Timeout



Prend des captures d'écran et enregistre des vidéos d'écrans de poste de travail.

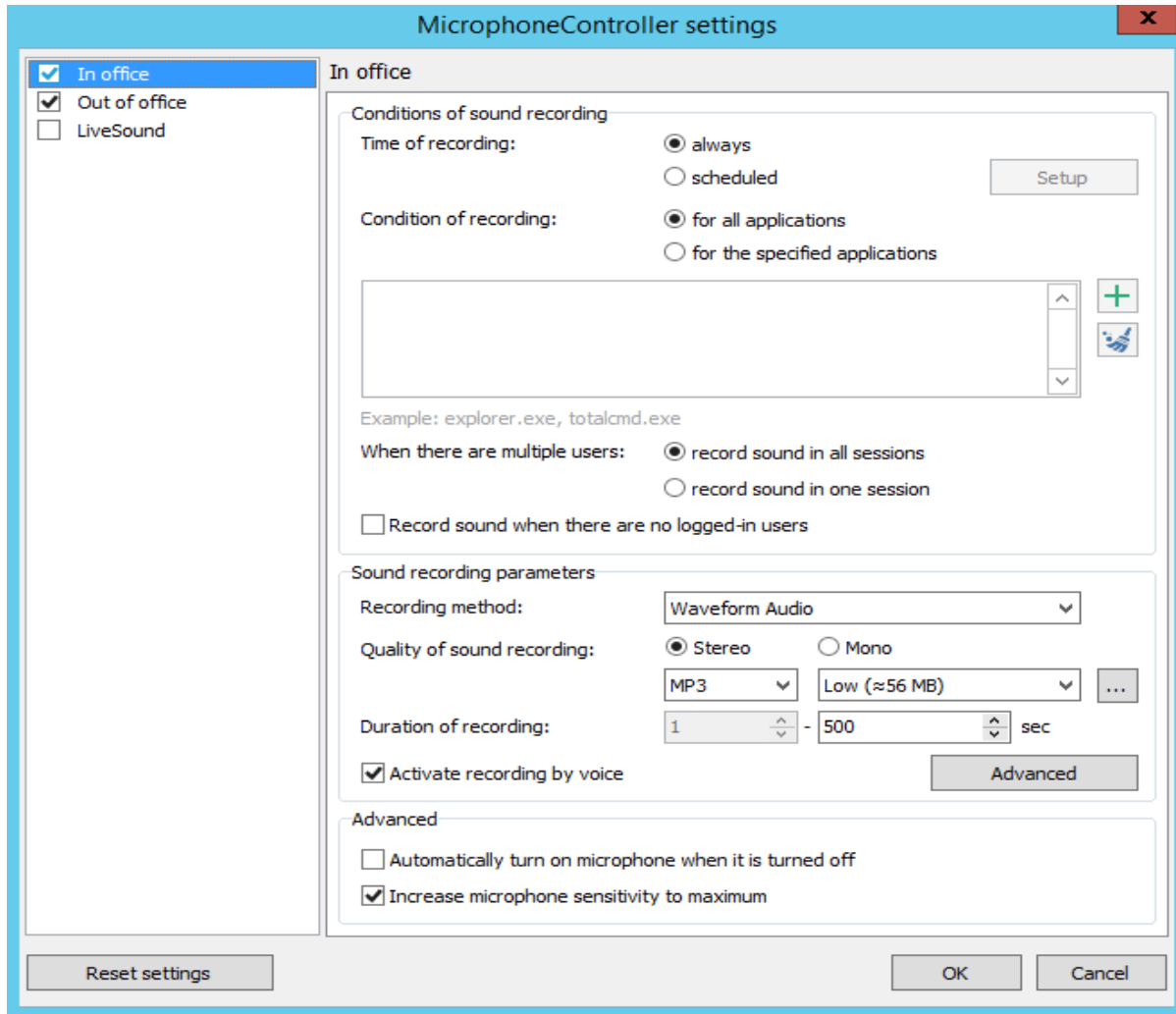
Fonctionne en plusieurs modes ::

Enregistrement vidéo :

Enregistrement continu des actions des employés sur les ordinateurs.

Les algorithmes de compression peuvent contenir 8 heures de "film" continu en seulement 300 mégaoctets.

Microphone Controller



Enregistre les conversations des employés au bureau et lors de voyages d'affaires via n'importe quel microphone détecté, intégré ou branché :

- *Enregistrement continue ;*
- *L'enregistrement peut être déclenché par un lancement de programme/processus ;*
- *L'enregistrement peut être déclenché par la parole humaine ;*
- *Diffusion sonore en direct.*

Analytical instruments: *Hardware report*

The screenshot displays the 'Reports - Analytic Console' interface. The left sidebar shows a tree view with categories: 'Reports on software', 'Reports on hardware', and 'System reports'. Under 'Reports on hardware', 'Hardware installation history' is selected. The main content area shows a report titled 'Hardware installation history' for a user. The report lists various hardware components installed on 24.06.2019, including CPU, Memory, Monitors, Display adapters, Storage devices, and Sound devices. A table at the bottom shows the 'Hardware installation history (period: not set)' with columns for Date and Name.

Hardware installation history

USER

CPU

+ 24.06.2019 Intel(R) Xeon(R) CPU E5606 @ 2.13GHz

Memory

+ 24.06.2019 (1 GB)

Monitors

+ 24.06.2019 [Redacted]

Display adapters

+ 24.06.2019 VMware SVGA 3D (Microsoft Corporation - WDDM)

Storage devices

+ 24.06.2019 VMware Virtual disk SCSI Disk Device (24 GB)

Sound devices

+ 24.06.2019 Virtual Audio Cable

Page 5 from 6 10.09.2019 10:59:59

Hardware installation history (period: not set)

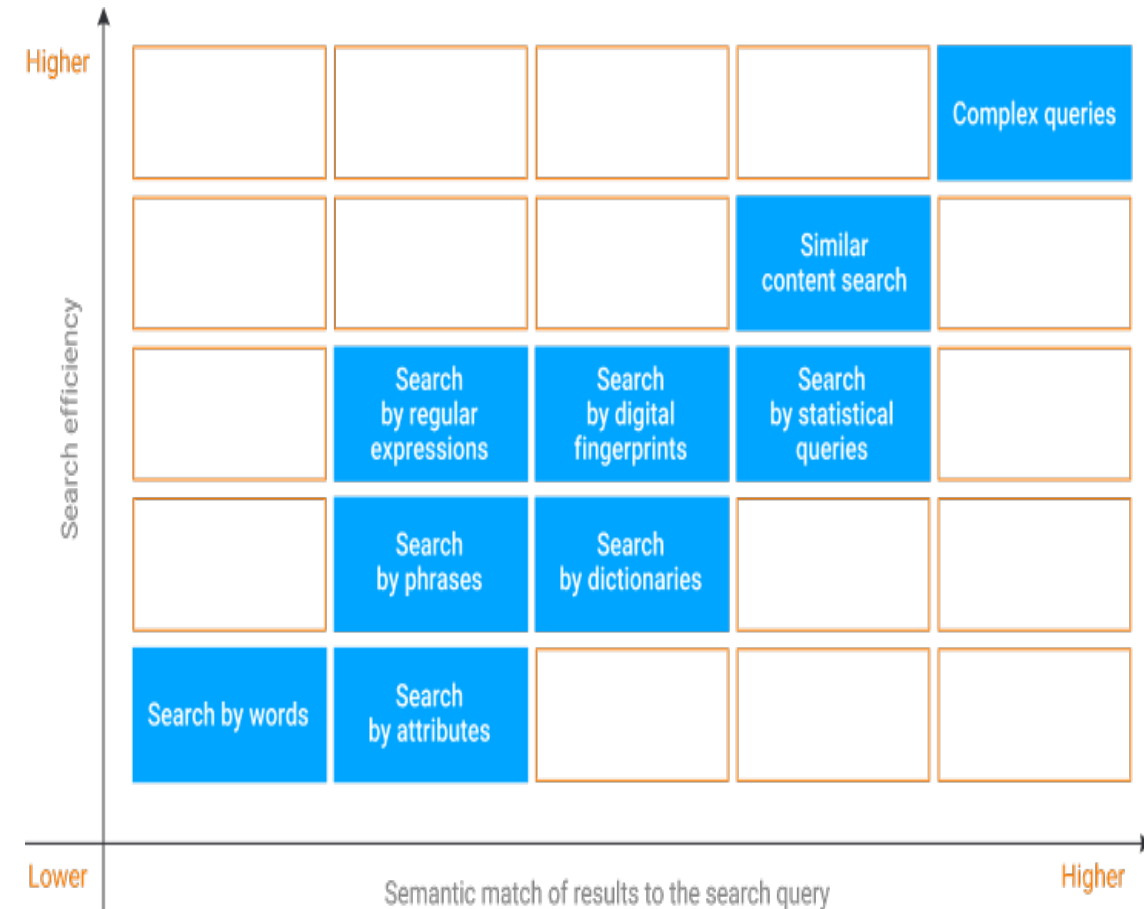
Date	Name
+ 24.06.2019	Virtual Audio Cable
+ 24.06.2019	WAN Miniport (SSTP)

ANALYTICAL INSTRUMENTS

Afin de détecter les activités suspectes dans les données capturées, Risk Monitor utilise 7 types de recherche :

- Recherche par mots clés
- Recherche d'expressions
- Recherche avec des dictionnaires
- Recherche d'attributs
- Recherche de contenu similaire
- Recherche à l'aide d'expressions régulières
- Recherche à l'aide d'empreintes digitales

Le système vous permet de combiner des requêtes uniques pour créer des algorithmes de recherche complexes qui forment les politiques de sécurité de l'information.



Ces capacités analytiques de SearchInform Risk Monitor permettent à un responsable de la sécurité de l'information de contrôler jusqu'à 1 000 à 1 500 employés.

SEARCHINFORM PRODUITS.

PREUVE DE CONCEPT POC GRATUIT



30 jours



*Plus que 1000
licenses*



Formation



Test de solution multiple



*Ingénieur dédié et responsable de la
mise en œuvre*

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Wi-Fi | Réseaux



Nous Contacter

www.hafs-afrique.com

West Africa | Côte d'Ivoire

+225 07 89 82 56 49 | 07 87 57 64 11

sales@hafs-afrique.com

Maroc

+212 52 24 49 937

sales@hafs-networks.com

North & Central Africa | France

+33 09 73 89 20 39 | 06 24 12 27 05

sales@hafs-networks.com