

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

NỀN TẢNG GIẢM THiểu RỦI RO NỘI BỘ



www.searchinform.com

1995 Công ty được thành lập



Các văn phòng và đối tác trên toàn thế giới

khách hàng trên hơn 20 nước
Hơn 3 000+

8 Sản phẩm và dịch vụ để bảo vệ dữ liệu một cách toàn diện



2019 SearchInform bắt đầu cung cấp các dịch vụ giám sát



2020 Giải pháp của SearchInform trên nền tảng đám mây đã được công bố

2018-2020

Một loạt các buổi RoadShow của SearchInform

Đã được tổ chức

ở Mỹ Latinh, Trung Đông và Bắc Phi, Nam Phi, Ấn Độ và Indonesia

32 số lần thắng kiện của khách hàng trong các vụ xét xử hình sự

2017 Phần mềm của searchinform lọt vào danh sách **Gartner Magic Quadrant**



2010 **Mở Trung tâm đào tạo**

Tập đoàn Radicati đã đưa SearchInform vào trong nghiên cứu "Thị trường chống thất thoát dữ liệu doanh nghiệp, 2017-2021"

SẢN PHẨM VÀ DỊCH VỤ



SearchInform DLP
(Chống thất thoát dữ liệu)

Trang 4



SearchInform Risk Monitor
(Giám sát rủi ro)

Trang 4-11



SearchInform ProfileCenter
(Giải pháp phân tích profile)

Trang 12-13



SearchInform SIEM
(Giải pháp quản lý sự kiện và an ninh mạng)

Trang 14-15



SearchInform FileAuditor
(Giải pháp giám sát hệ thống file)

Trang 16-17



SearchInform TimeInformer
(Giải pháp giám sát giờ làm việc)

Trang 18-19



SearchInform Services
(Dịch vụ)

Trang 20-22

© SearchInform DLP

Bảo vệ công ty khỏi rò rỉ thông tin bí mật, kiểm soát lưu trữ và truyền tải dữ liệu.

Giám sát tất cả các kênh truyền dữ liệu phổ biến, phân tích thông tin, phát hiện và ngăn chặn vi phạm, cung cấp báo cáo cho người chuyên trách.

SEARCHINFORM DLP GIÚP DOANH NGHIỆP THEO NHIỀU CÁCH

- Bảo vệ thông tin bí mật khỏi bị rò rỉ trong quá trình lưu trữ, sử dụng và truyền tải
- Mã hóa dữ liệu để ngăn không cho dữ liệu đó được sử dụng bên ngoài công ty
- Kiểm soát truy cập từ xa và các công cụ ảo hóa (TeamViewer, RAdmin, RDP)
- Báo cáo các sự kiện bất thường trong mạng, chẳng hạn như sao chép dữ liệu vào thiết bị lưu trữ di động hoặc xóa một số lượng lớn dữ liệu
- Tạo điều kiện thuận lợi cho việc kiểm kê phần mềm và phần cứng

⊕ SearchInform Risk Monitor

SearchInform cung cấp cách tiếp cận toàn diện để giám sát nội bộ bằng cách mở rộng giải pháp DLP và kết hợp hai khái niệm mạnh mẽ: phòng ngừa sự cố và giảm thiểu mối đe dọa nội bộ.

Các công cụ giảm thiểu mối đe dọa nội bộ và xác định rủi ro nội bộ bảo vệ doanh nghiệp của bạn khỏi những tổn thất về tài chính và danh tiếng do các mối đe dọa đó gây ra.

GIẢI PHÁP CỦA SEARCHINFORM TRÊN ĐÁM MÂY

Các doanh nghiệp không phải lựa chọn giữa bảo mật, khả năng sử dụng và chi phí vì giải pháp có thể được triển khai trên đám mây. Không yêu cầu phần cứng đặc biệt: hệ thống thu thập, xử lý và lưu trữ dữ liệu trong môi trường ảo. Mô hình triển khai như vậy sẽ phù hợp với các công ty không có cơ sở hạ tầng CNTT riêng, văn phòng của họ đặt tại các thành phố khác nhau, có số lượng lớn nhân viên làm việc từ xa.

GIẢI PHÁP MỞ RỘNG:

- Phát hiện các sự cố gián điệp liên quan đến gian lận và trục lợi của công ty
- Kiểm soát yếu tố con người và dự đoán rủi ro nhân sự
- Tạo điều kiện thuận lợi cho các quy trình điều tra và tuân thủ quy định
- Hoạt động như một hệ thống cảnh báo sớm phát hiện các mối đe dọa tiềm ẩn hoặc dấu hiệu vi phạm và cảnh báo những rủi ro có thể xảy ra

Risk Monitor cung cấp cho bạn bộ công cụ tự động có độ chính xác cao để giám sát nhân viên, đánh giá rủi ro và kiểm toán nội bộ, đảm bảo rằng các chính sách của công ty được tuân thủ bởi các cơ quan quản lý và đánh giá sự phù hợp mức độ bảo mật của công ty với các tình hình cấp thiết hiện nay.

Giải pháp tạo điều kiện thuận lợi cho việc tạo ra chương trình quản lý rủi ro.

Mục tiêu của chương trình quản lý rủi ro tương ứng là xem xét các hoạt động để xác định chắc chắn rằng các hoạt động này đáp ứng được các yêu cầu đã thiết lập và các hoạt động đang được thực hiện theo kế hoạch.

Mặc dù những thiệt hại ngẫu nhiên do hoạt động của con người thường không lường trước được, nhưng giải pháp SearchInform có thể bảo vệ một công ty trước các sự cố nội bộ. Khung (framework) quản lý rủi ro là cốt lõi của phần mềm SearchInform, giúp dự đoán gian lận trong doanh nghiệp và ngăn ngừa tổn thất tài chính.

MỤC TIÊU



Thu thập thông tin chi tiết về các hoạt động của người dùng để mô phỏng lại từng bước vụ việc vi phạm



SBảo vệ công ty trước những rủi ro về nhân sự và dự đoán các hành vi của nhân viên



Tạo một kho lưu trữ thông tin bị chặn, tạo điều kiện thuận lợi cho việc tuân thủ quy định và nâng cao chính sách bảo mật để giảm thiểu rủi ro



Giúp tăng năng suất của nhân viên và hỗ trợ quản lý lòng trung thành, tinh thần tập thể



Cảnh báo về mối đe dọa tiềm ẩn trước khi sự cố xảy ra, do đó thúc đẩy văn hóa an ninh doanh nghiệp và nâng cao nhận thức về những mối đe dọa nội bộ

NHẬP THÔNG TIN

Giải pháp của SearchInform bao gồm các mô-đun, mỗi mô-đun kiểm soát kênh dữ liệu riêng của mình.





MailController

Ghi lại tất cả thư đi và đến được gửi qua người dùng và các dịch vụ web, bao gồm Gmail, Yahoo, Hotmail, v.v. Nó phát hiện việc gửi tin nhắn đến các e-mail riêng và địa chỉ e-mail của các đối thủ cạnh tranh và chặn việc truyền các tin nhắn nếu nội dung của chúng xâm phạm đến dữ liệu bí mật của công ty.



MonitorController

Chụp ảnh màn hình và quay video về hoạt động trên màn hình. Bổ sung cảnh quay hình ảnh và video với thông tin mới nhất về các cửa sổ đang mở và các quy trình đang diễn ra. Nếu cần, hiển thị thông tin trong thời gian thực. Chụp ảnh nhanh để xác định kẻ xâm nhập.



IMController

Theo dõi các cuộc trò chuyện, lịch sử tin nhắn, cuộc gọi và danh sách liên hệ trong các trình duyệt nhắn tin: Skype, WhatsApp, Telegram, Viber, Lync, Gadu-Gadu, XMPP, v.v. Theo dõi thư từ qua các dịch vụ web trên mạng xã hội, chẳng hạn như Facebook, Google+, LinkedIn, v.v.



HTTPController

Ghi lại và lập chỉ mục các tệp và tin nhắn được gửi qua HTTP / HTTPS. Nếu cần, nó sẽ chặn lưu lượng truy cập web, bao gồm các tin nhắn qua mạng, dịch vụ đám mây, mail, blog, diễn đàn, mạng xã hội và truy vấn tìm kiếm. Duy trì chức năng giám sát thường xuyên ngay cả khi nhân viên sử dụng ẩn danh.



ProgramController*

Thu thập dữ liệu về hoạt động của người dùng trong ngày và thời gian dành cho các ứng dụng, chương trình và trên các trang web. Tự động xác định xem một nhân viên đang làm việc hay vừa khởi động chương trình để biết là đang làm việc gì đó. Phân loại các tài nguyên web: hẹn hò, âm nhạc, mua sắm, tin tức, v.v.



CloudController

Kiểm soát các tệp đã nhận, tải lên và lưu trữ trong kho lưu trữ đám mây. Theo dõi các dịch vụ lưu trữ đám mây và chia sẻ tệp: Google Docs, Office 365, Evernote, iCloud Drive, SharePoint, Dropbox, Amazon S3, DropMeFiles, v.v. Chặn các tệp được gửi và nhận thông qua các ứng dụng TeamViewer, RealVNC, Radmin, LiteManager.



FTPController

Kiểm tra thường xuyên lưu lượng (traffic) (FTP) và được mã hóa (FTPS) và thông báo cho người điều hành về các sự cố hoặc chặn kết nối.



DeviceController

Phát hiện và chặn dữ liệu được truyền sang ổ đĩa flash, ổ cứng ngoài, CD / DVD, qua RDP và máy ảnh. Tự động mã hóa dữ liệu được ghi vào ổ đĩa flash. Phát hiện và nhận dạng điện thoại thông minh được kết nối với PC (Android, Apple, BlackBerry, Windows Phone), phân tích nội dung của chúng khi được kết nối ở chế độ ổ đĩa. Kiểm soát quyền truy cập của thiết bị vào PC.



MicrophoneController

Sử dụng bất kỳ micrô nào được phát hiện để ghi lại các cuộc nói chuyện trong và ngoài văn phòng. Bật ghi âm - ngay cả trước khi người dùng đăng nhập - khi giọng nói được phát hiện hoặc khi các quy trình và chương trình nhất định, như được chỉ định trong chính sách bảo mật liên quan, được khởi chạy. Luồng âm thanh có thể được chuyển đổi thành văn bản, cũng được kiểm tra theo các chính sách bảo mật đã chỉ định

*Giúp bạn giám sát hiệu suất của nhân viên từ xa



Keylogger

Phát hiện các lần nhấn phím và dữ liệu được sao chép vào bộ nhớ đệm. Chặn dữ liệu đăng nhập và mật khẩu để tạo điều kiện thuận lợi cho việc theo dõi các tài khoản được duy trì trên các tài nguyên web có thể gây hại. Xác định người dùng đã nhập mật khẩu trên bàn phím của họ để truy cập tài liệu được mã hóa.



PrintController

Kiểm tra nội dung của tài liệu được gửi để in (các tệp văn bản chỉ được sao chép đơn giản và các bản quét tài liệu được chặn dưới dạng 'dấu vân tay' kỹ thuật số với nội dung văn bản của chúng được nhận dạng). Phát hiện các tài liệu được chứng thực bằng con dấu và giám sát việc in các biểu mẫu phát hành được kiểm soát.

CONTROL CENTER (TRUNG TÂM GIÁM SÁT)

DataCenter (Trung tâm dữ liệu)

Quản lý chỉ mục sản phẩm và cơ sở dữ liệu, giám sát tình trạng hệ thống và kết nối với các hệ thống của bên thứ ba, như AD, SOC, máy chủ thư đi (outgoing mail server). Người dùng DataCenter có thể cấu hình quyền truy cập.

AlertCenter (Trung tâm cảnh báo)

Đây được coi là "Viện nghiên cứu" của hệ thống, nơi các chính sách bảo mật được thiết lập. Nó bao gồm hơn 250 chính sách bảo mật được cấu hình sẵn có thể được chỉnh sửa. Giải pháp này giúp bạn có thể tạo các quy tắc tùy chỉnh về quét và chặn dữ liệu đã được phát hiện, cấu hình lịch kiểm tra và gửi thông báo.

Bạn có thể xem các sự cố trong bảng điều khiển AlertCenter trên PC công ty của người có trách nhiệm hoặc qua giao diện web, có thể truy cập từ máy tính xách tay, máy tính bảng, điện thoại thông minh.

The screenshot shows the AlertCenter Administrator interface. The main window displays 'Security policies \ Case 5' with a table of incidents. Below the table, there is a search result for a document named 'bank_statement_1Feb2018.pdf'. The document content is displayed, showing a list of transactions with columns for Date, Description, and Amount.

Date	Description	Amount
1/9/2018	Transfer to TechSol	400.00
1/9/2018	Payment for the maintenance of network and computers	700.00
1/11/2018	Payment for the service.com use	2,200.00
1/11/2018	Transfer to JAMES & Co	8,000.00
1/13/2018	Payment for the transport of goods	2,289.50
1/16/2018	Payment of transportation charges	3,000.00
1/18/2018	Payment for the service.com use	4,000.00

Chính sách bảo mật và kết quả tìm kiếm trong AlertCenter

Analytic Console (Bảng điều khiển phân tích)

Mục tiêu của nó là duyệt qua dữ liệu bị chặn và phân tích nó cũng như giám sát các hoạt động trực tuyến của người dùng. Các thuật toán tìm kiếm khác nhau và các mẫu báo cáo cài đặt trước được chuyên gia xử lý.

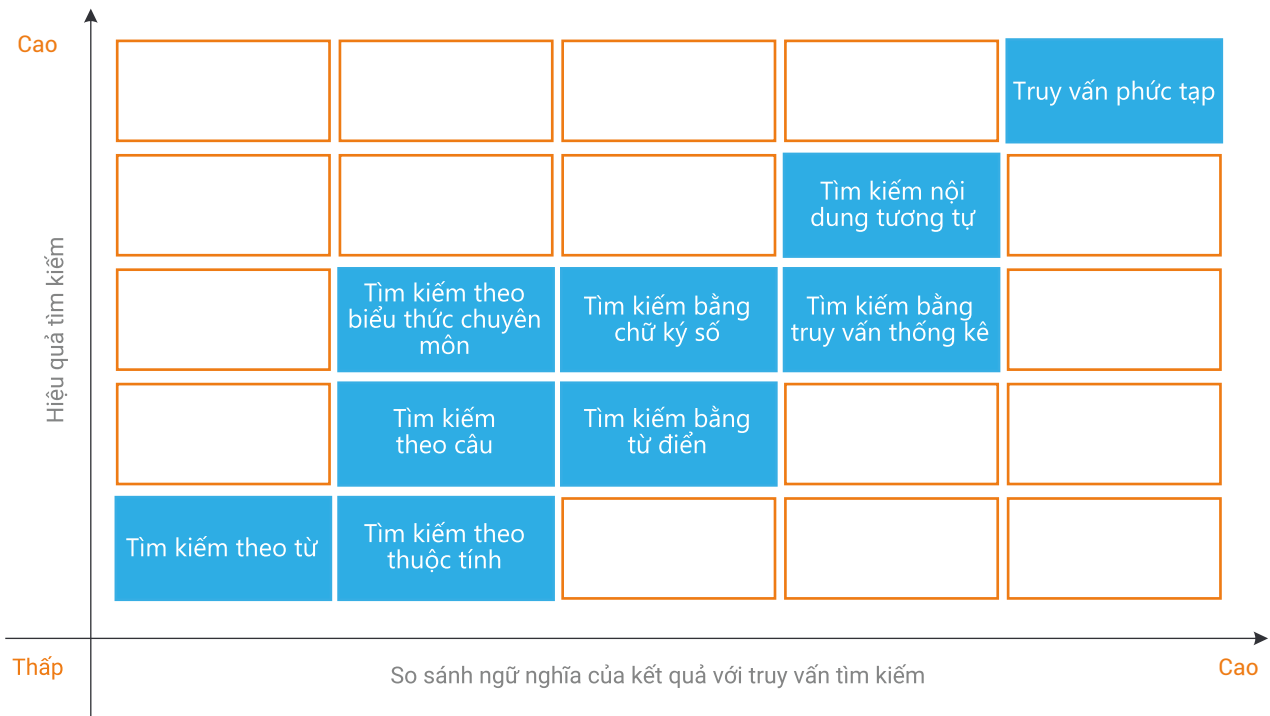
Các báo cáo được tạo trong Bảng điều khiển phân tích có sẵn trong phiên bản web của bảng điều khiển.

ANALYTICAL CAPABILITIES (KHẢ NĂNG PHÂN TÍCH)

Để thực hiện các chức năng của mình một cách hiệu quả, các chuyên gia phải có khả năng kiểm soát toàn diện trên tất cả các kênh liên lạc cũng như có đủ chức năng để tìm kiếm thông qua dữ liệu được thu thập được và phân tích nó. Một mô-đun phân tích mạnh mẽ có các tùy chọn tìm kiếm khác nhau và phân tích đồ họa và âm thanh tự động cho phép chỉ một chuyên gia có thể kiểm tra công việc của vài nghìn nhân viên.

Text analysis (Phân tích văn bản)

Một loạt các thuật toán cung cấp khả năng xác minh chuyên sâu các tin nhắn văn bản và tài liệu. Có các công nghệ tìm kiếm độc đáo như Tìm kiếm nội dung tương tự (Similar Content Search) hoặc Truy vấn phức tạp (Complex Queries). Thuật toán "Tìm kiếm nội dung tương tự" có thể xác định được các tài liệu bí mật ngay cả khi chúng đã được chỉnh sửa, có nghĩa là kết quả tìm kiếm sẽ bao gồm các tài liệu phù hợp với truy vấn về mặt ngữ nghĩa thay vì chỉ về mặt câu chữ. Các "Truy vấn phức tạp" cho phép người dùng xây dựng các thuật toán tìm kiếm nâng cao bằng cách sử dụng các truy vấn đơn giản được kết hợp một cách hợp lý bởi các toán tử AND, OR và NOT.



Graphics analysis (Phân tích đồ họa)

Hệ thống xác định các loại hình ảnh lưu hành trong công ty: PDF, ảnh chụp hoặc bản sao scan - và phân loại tệp hình ảnh cho phù hợp. Hệ thống OCR - Optical Character Recognition (Nhận dạng ký tự quang học) tích hợp xác định các tài liệu theo các mẫu cụ thể: hộ chiếu, thẻ ngân hàng, giấy phép lái xe, v.v. Công nghệ này cho phép tìm kiếm dữ liệu cá nhân, tài chính và bất kỳ dữ liệu nhạy cảm nào khác trong kho lưu trữ, thậm chí được truyền dưới dạng tài liệu scan.

Audio analysis (Phân tích âm thanh)

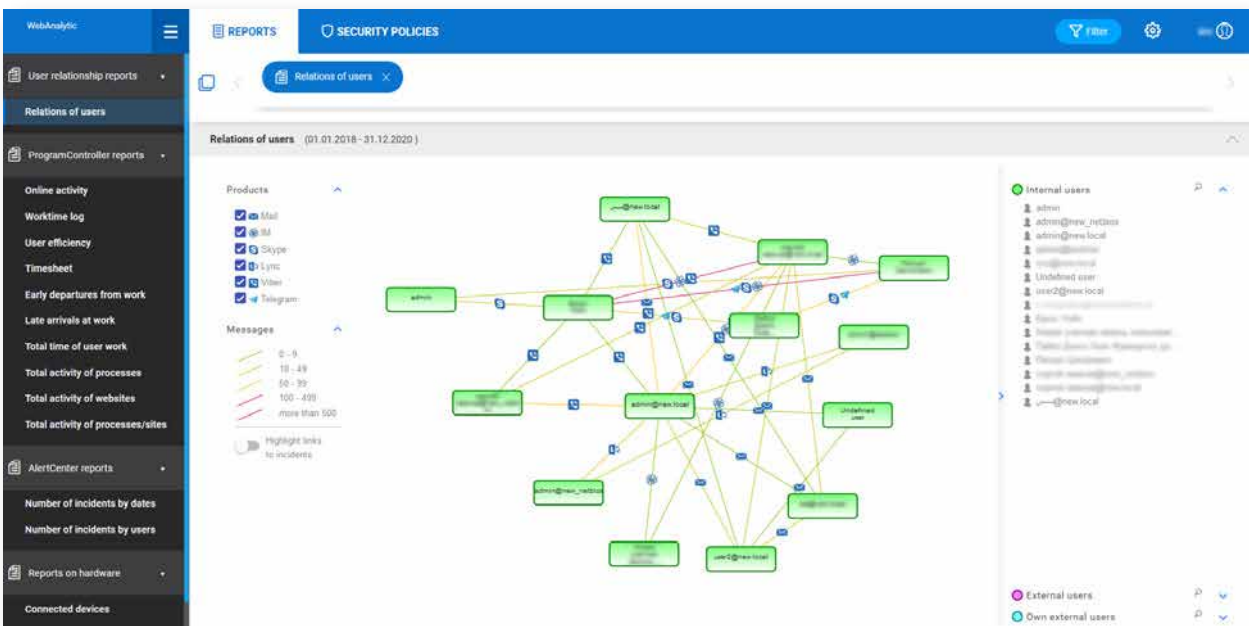
Giải pháp SearchInform chuyển đổi bản ghi âm thanh thành văn bản và kiểm tra xem bản ghi có tuân thủ các chính sách bảo mật hay không. Hệ thống có tùy chọn để bật ghi âm khi phát hiện giọng nói hoặc khi một số quy trình hoặc chương trình nhất định, như được chỉ định trong chính sách bảo mật liên quan, được khởi chạy.

REPORTS & UEBA (BÁO CÁO & PHÂN TÍCH HÀNH VI NGƯỜI DÙNG VÀ THỰC THỂ)

Phần mềm SearchInform hiển thị trực quan tất cả các sự kiện và kết nối trong công ty dưới dạng báo cáo - thông qua Bảng điều khiển phân tích (Analytic Console) và giao diện web. Cấu hình mặc định bao gồm hơn 30 mẫu cơ bản. Trình hướng dẫn báo cáo cho phép người dùng tạo các báo cáo tùy chỉnh không bị giới hạn bởi bất kỳ tiêu chí nào.

RelationsChart report (Báo cáo biểu đồ quan hệ)

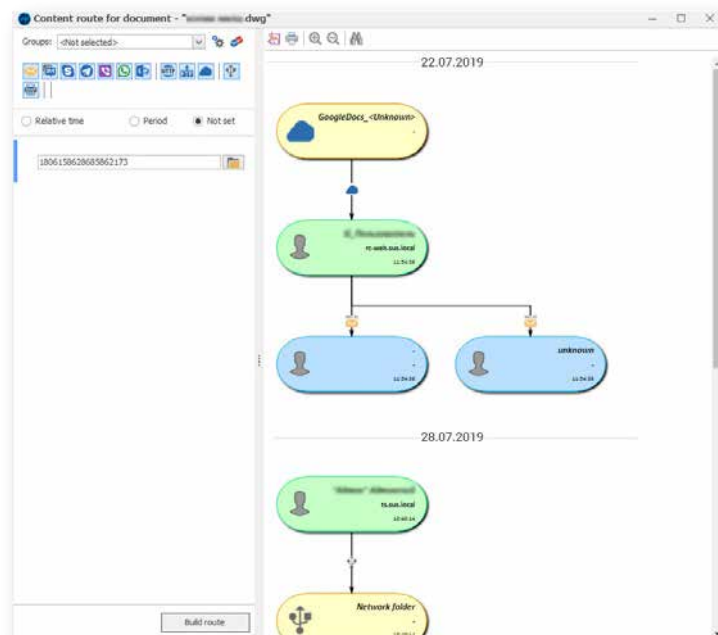
Thể hiện các kết nối giữa nhân viên với nhân viên, nhân viên với bên thứ ba dưới dạng biểu đồ quan hệ. Trực quan hóa các hoạt động của người dùng trên tất cả các kênh liên lạc hoặc trong một đường dây liên lạc cụ thể. Tạo điều kiện thuận lợi cho các cuộc điều tra của công ty.



Đồ thị quan hệ Bảng điều khiển phân tích

Content routing report (Báo cáo định tuyến nội dung)

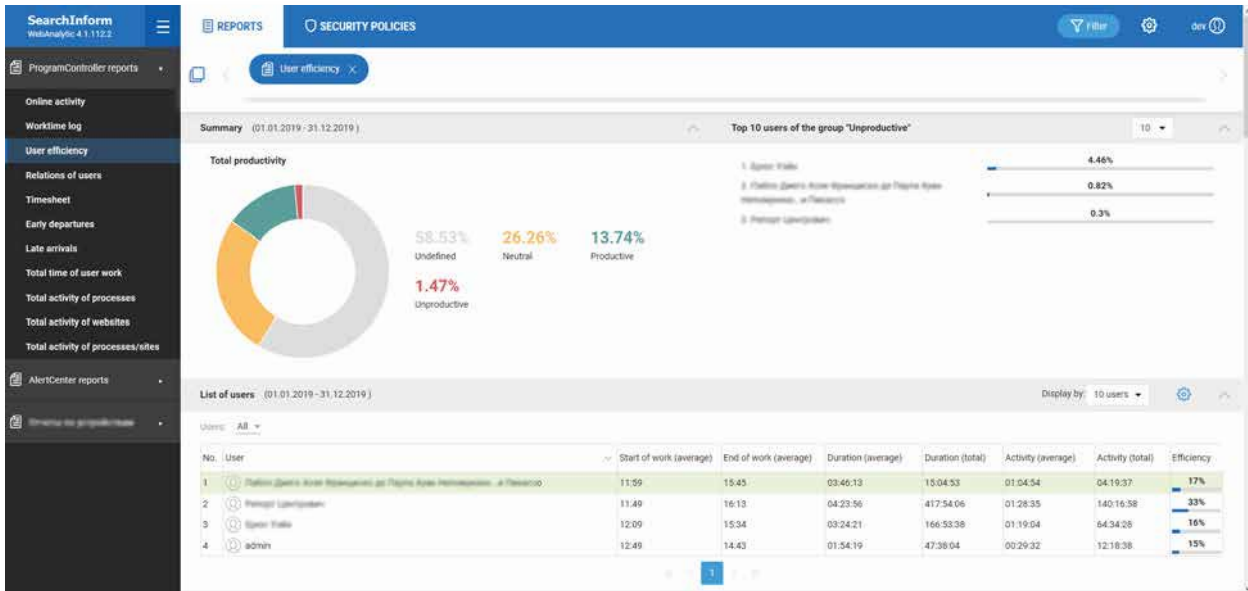
Làm cho tất cả các chuyển động tài liệu giữa người gửi và người nhận thông qua các kênh liên lạc nội bộ và bên ngoài trở nên hoàn toàn minh bạch. Cung cấp khả năng xác định nhanh chóng tác giả của tài liệu cũng như nguồn của thông tin tương ứng và các đường dẫn phân phối tài liệu.



Định tuyến nội dung

User productivity report (Báo cáo hiệu suất người sử dụng)

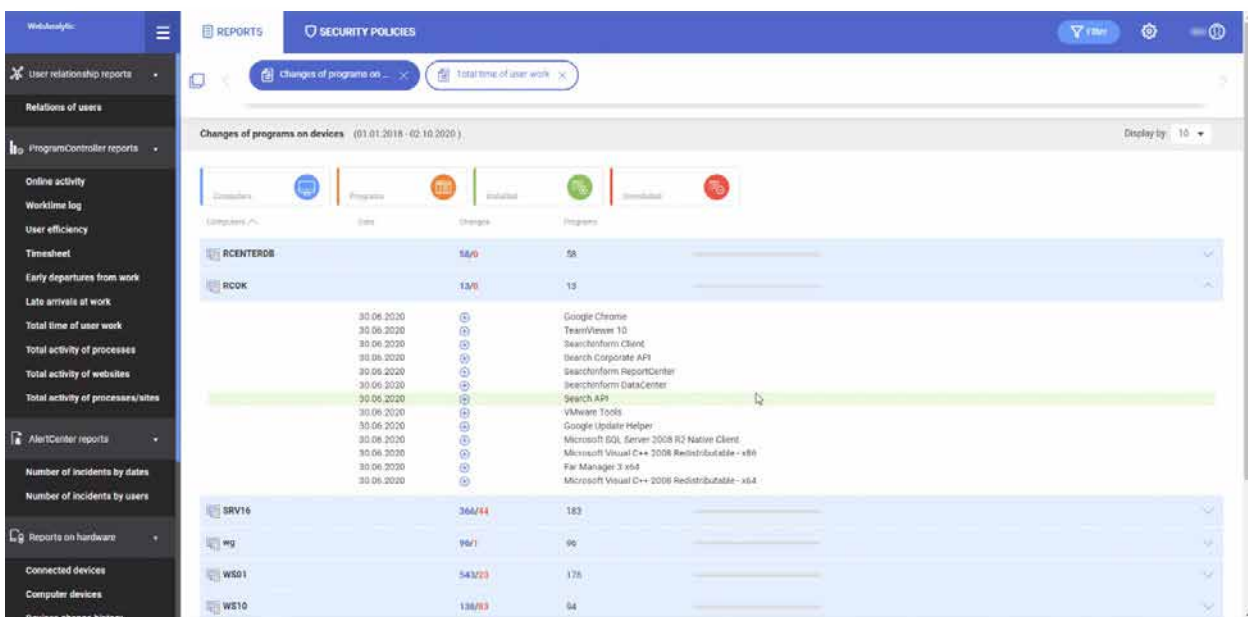
Hiển thị tổng thể hiệu suất của nhân viên công ty trong biểu đồ và xếp hạng. Nó phát hiện tần suất nhân viên đi làm sớm/ngủi làm và những người thường xuyên đi làm muộn. Trực quan hóa hiệu suất của người dùng trong tuần làm việc ở định dạng lịch.



Báo cáo hiệu suất của người dùng

Software and hardware report (Báo cáo phần cứng và phần mềm)

Báo cáo mọi thay đổi đối với phần cứng đã được lắp đặt và các thiết bị được kết nối. Điều này tạo điều kiện thuận lợi cho việc kiểm kê và bảo vệ chống trộm cắp thiết bị hoặc thay thế thiết bị trái phép. Báo cáo phần mềm thu thập dữ liệu về hoạt động cài đặt và gỡ cài đặt phần mềm.



Báo cáo phần cứng và phần mềm

ƯU ĐIỂM

Dễ dàng triển khai mà không cần thay đổi cấu trúc mạng

Các chuyên gia CNTT của công ty khách hàng có thể cài đặt SearchInform trong vòng vài giờ. Quá trình cài đặt không cản trở hoạt động của hệ thống thông tin nội bộ của công ty.

Một mô-đun phân tích mạnh mẽ

Cung cấp các giải pháp nhanh chóng và linh hoạt để định cấu hình cảnh báo và phân tích luồng dữ liệu mà không cần thuê chuyên gia của bên thứ ba. Với sự trợ giúp của sản phẩm SearchInform, một chuyên gia có thể kiểm soát công việc của hàng nghìn nhân viên.

Các công cụ để điều tra sự cố theo từng bước

Ghi lại các cuộc trò chuyện và ghi lại nội dung trên màn hình trong thời gian thực, giám sát đầu vào bàn phím và tạo video bằng webcam - các thành phần tích hợp của hệ thống này giúp theo dõi từng bước vi phạm.

Mô hình triển khai đám mây

Các thành phần của Giám sát rủi ro (Risk Monitor) có thể được triển khai trên đám mây (có thể sử dụng đám mây SearchInform hoặc bất kỳ dịch vụ đám mây nào của bên thứ ba) mà không can thiệp vào chức năng của hệ thống. Cách bảo vệ dữ liệu này tiết kiệm chi phí và thời gian.

Mô phỏng mối quan hệ giữa các nhân viên

Biểu đồ quan hệ tương tác là một công cụ hỗ trợ trực quan tốt thể hiện các vòng kết nối xã hội và đường dây liên lạc liên quan đến cả nhân viên của công ty và những người liên hệ bên thứ ba của họ.

Kiểm soát truy cập từ xa

Giải pháp SearchInform bảo vệ dữ liệu truyền qua môi trường ảo và các công cụ điều khiển từ xa. Việc giám sát được thực hiện ở cả cấp bộ nhớ tạm, kết nối thiết bị lưu trữ ảo và ở cấp các tính năng phần mềm cụ thể (ví dụ: truyền qua menu ngữ cảnh (context menu) của TeamViewer).

Định tuyến nội dung tài liệu

Nó thể hiện sự di chuyển của các tài liệu, cho biết người gửi và người nhận, cũng như các kênh liên lạc được sử dụng để truyền dữ liệu.

Giải pháp toàn diện

Cấu trúc nhiều thành phần sẽ cung cấp cho bạn các giải pháp đầy đủ từ giám sát toàn diện đa kênh về rò rỉ dữ liệu hay chỉ là kết hợp một số mô-đun tùy chọn dựa trên nhu cầu của bạn, trong trường hợp đó chi phí sẽ thấp hơn đáng kể.

Các giải pháp an ninh cho các công ty phân tán về mặt địa lý

Tại các văn phòng chi nhánh ở xa với số lượng máy tính nhỏ và có kênh liên lạc đến trụ sở chính, nơi không thể triển khai một hệ thống chính thức, thì dữ liệu sẽ được lọc, xử lý và mã hóa cục bộ trước khi chuyển đến máy chủ.

Các giải pháp có thể hoạt động trên hệ điều hành Linux

Sản phẩm SearchInform có thể hoạt động trên các hệ điều hành phổ biến nhất hiện nay

Tích hợp với các sản phẩm SearchInform khác

Giải pháp SearchInform được tích hợp liền mạch với SIEM, ProfileCenter, FileAuditor và Database Monitor, giúp tăng mức độ bảo mật thông tin và nhận thức rủi ro của công ty, giảm thời gian phản hồi sự cố, giúp điều tra đầy đủ các hành vi phạm.

Cơ quan thực hiện và Trung tâm đào tạo

Kinh nghiệm thực tế của chúng tôi với hơn 3.000 công ty trong các ngành khác nhau cho phép chúng tôi nhanh chóng tạo ra các bộ chính sách bảo mật đặc thù tập trung vào các nhiệm vụ có liên quan và ngành nghề kinh doanh cụ thể của khách hàng.

Kho lưu trữ các thông tin bị chặn

Tạo điều kiện thuận lợi đáng kể cho việc xây dựng lại chuỗi sự kiện và cho phép một công ty tiến hành điều tra, truy cứu.

Giám sát lưu trữ dữ liệu

Hệ thống sẽ kịp thời phát hiện sự hiện diện của thông tin bí mật ở các vị trí không được thiết kế để lưu trữ.

SearchInform ProfileCenter

74% các công ty phát hiện ra rằng nhân viên của mình làm các hoạt động không liên quan đến công việc trong giờ làm*

*Theo thống kê của SearchInform năm 2019

74%
SỰ CỐ

Mục tiêu của công ty là mô phỏng rủi ro, thấy trước hoạt động của nhân viên và ngăn ngừa các sự cố có thể xảy ra.

Vấn đề trên được giải quyết bởi ProfileCenter - bộ công cụ chẩn đoán non-test (không kiểm tra) giúp phân loại tính cách, dự báo hành vi, làm nổi bật điểm mạnh, điểm yếu và phát hiện xu hướng tội phạm.

PHÂN TÍCH PROFILE GIÚP GÌ CHO VIỆC KINH DOANH CỦA BẠN?

Phương pháp phân tích Profile được áp dụng trong kinh doanh để phát hiện các hoạt động gian lận, nâng cao kỹ thuật quản lý nhân sự, tăng doanh số bán hàng và đánh giá rủi ro do các đặc điểm tính cách các cá nhân có thể gây hại cho đồng nghiệp hoặc công ty.

ProfileCenter phát hiện:

- Xu hướng phạm tội
- Thái độ ẩn
- Cảm xúc cơ bản
- Đặc điểm tính cách chính, điểm mạnh và điểm yếu
- Ứng xử trong các tình huống xung đột
- Vai trò xã hội của nhân viên trong nhóm

SẢN PHẨM LÀM VIỆC NHƯ THẾ NÀO?

BƯỚC 1

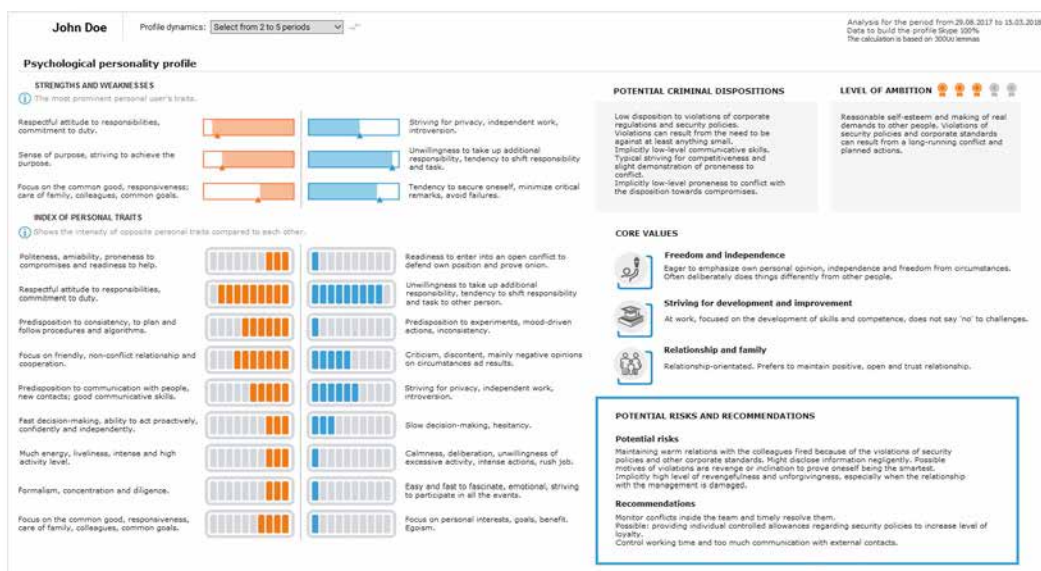
Hệ thống thu thập thư từ của nhân viên (qua email, tin nhắn, mạng xã hội)

BƯỚC 2

Phần mềm thực hiện phân tích hành vi và xác định mô hình tư duy dựa trên phân tích văn bản với hơn 70 tiêu chí

BƯỚC 3

Kết quả phân tích được hiển thị dưới dạng báo cáo cùng với khuyến nghị và cách giải quyết thực tế

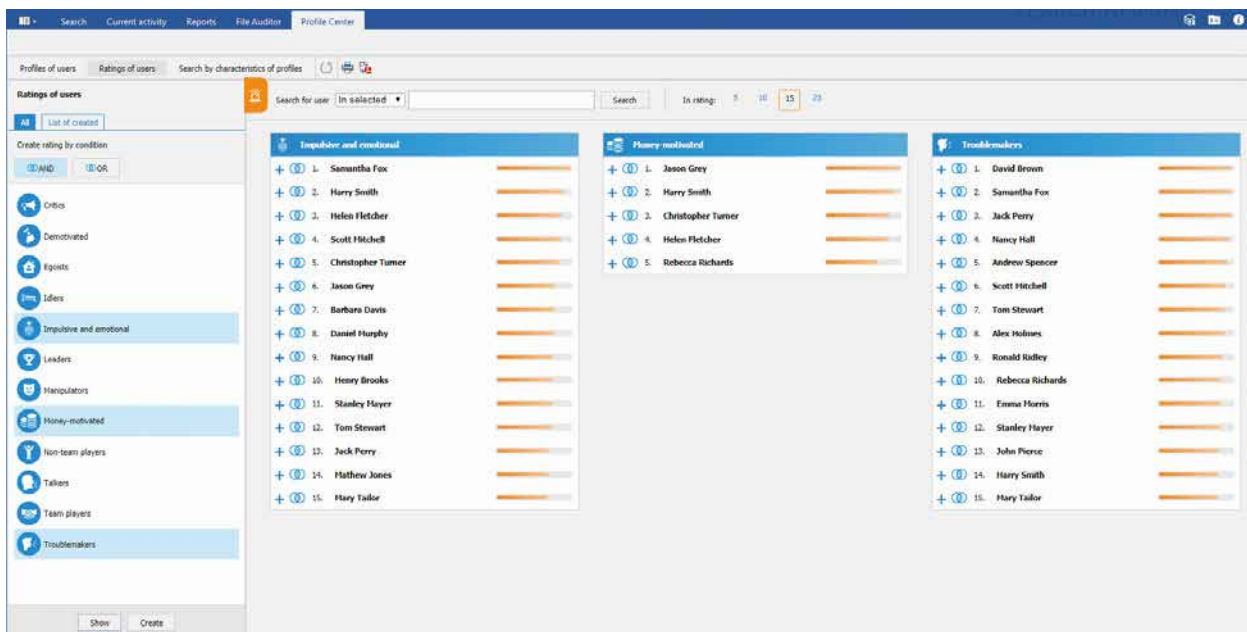


Hồ sơ cá nhân của một nhân viên

SẢN PHẨM GIÚP ĐƯA RA CÁC QUYẾT ĐỊNH DỄ DÀNG HƠN

Các khuyến nghị thực tế về:

- Những mẫu hành vi nào của nhân viên mà bạn nên chú ý
- Cách tạo một nhóm làm việc hiệu quả
- Nên thì thoải mái để ý hay luôn giám sát ai trong các tình huống cụ thể
- Mức độ an toàn khi cấp quyền truy cập vào thông tin bí mật, tài sản tài chính và các nguồn có giá trị
- Liệu công việc có phù hợp với nhân viên
- Cách nói chuyện, giao tiếp với nhân viên (nghiêm túc hay cởi mở,...)
- Đối với nhân viên việc khiển trách, nhắc nhở đã là đủ hay cần phải đào tạo lại hoặc kỷ luật.



Đánh giá nhân viên

ƯU ĐIỂM

- Giải pháp tự động cung cấp kết quả cho bạn một cách nhanh chóng, tiết kiệm chi phí thuê người lập và phân tích hồ sơ nhân viên
- Việc phân tích dữ liệu được thu thập bởi giải pháp bảo mật dữ liệu là thiết yếu hơn so với việc thông qua các bài kiểm tra đầu vào
- Theo dõi tính cách nhân viên trong cả một quá trình
- Không làm nhân viên phân tâm khỏi công việc, không làm các tình huống trở lên căng thẳng
- Phát hiện những thay đổi về tâm lý và thái độ làm việc của nhân viên trong nhóm

SearchInform SIEM

❖ HỆ THỐNG SIEM ĐỘT
PHÁ ĐẦU TIÊN

❖ TẠO CHÍNH SÁCH
TRONG HAI NHẤP CHUỘT

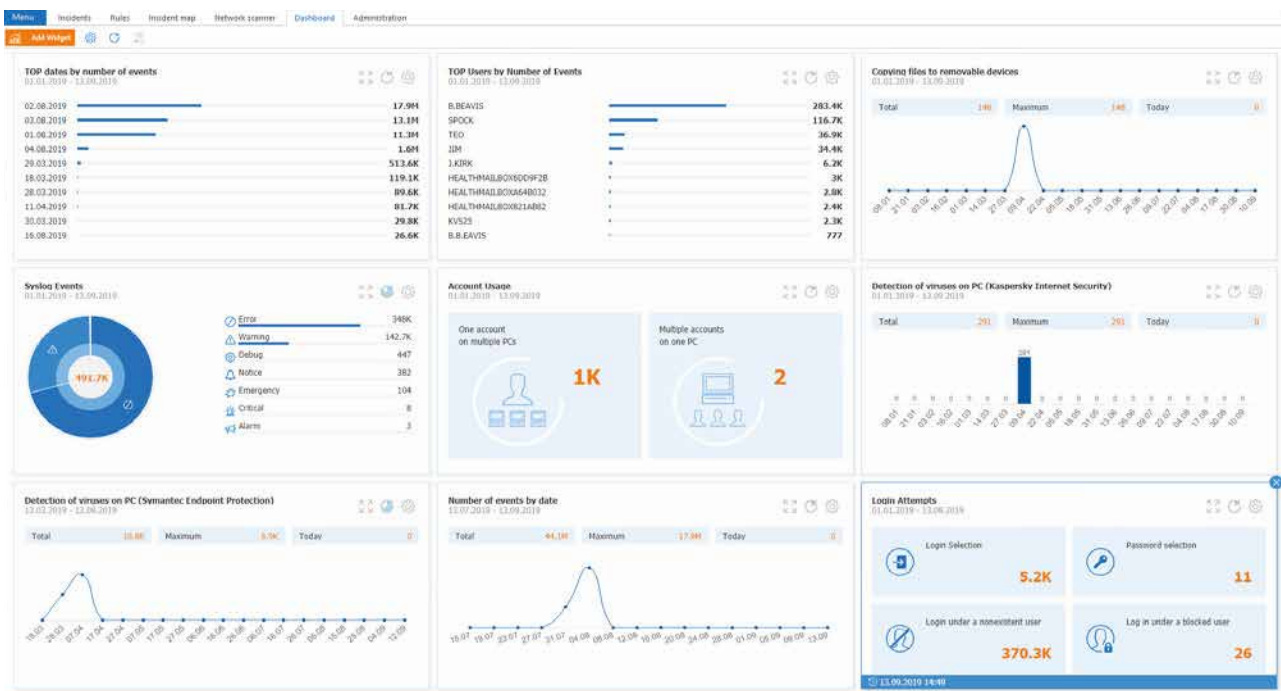
No.1

Cơ sở hạ tầng CNTT của một công ty bao gồm vô số các thành phần như: Tường lửa, hệ điều hành, email servers, cơ sở dữ liệu, thiết bị mạng.

Nhiều thành phần trong số này là mục tiêu thu hút những tin tặc, và cần phải được bảo vệ 1 cách đặc biệt.

Tự động giám sát các sự kiện an ninh

SearchInform SIEM là một hệ thống thu thập và phân tích các sự kiện an ninh theo thời gian thực, xác định các sự cố an toàn thông tin và ứng phó với chúng. Hệ thống tích lũy thông tin từ nhiều nguồn khác nhau, phân tích, ghi lại các sự cố và cảnh báo cho nhân viên quản trị.



Bảng điều khiển thống kê sự kiện

SearchInform SIEM phát hiện:

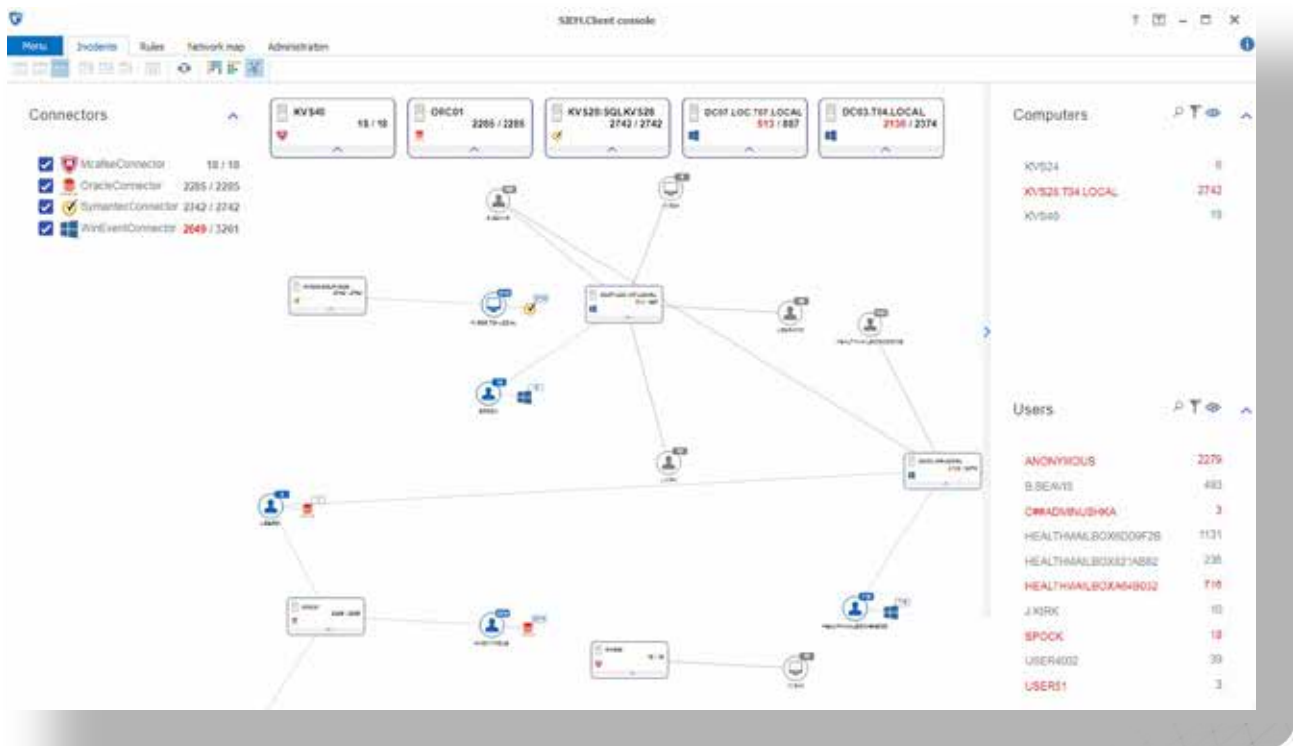
- Mối đe dọa do virus gây ra
- Truy cập trái phép vào dữ liệu
- Đoán mật khẩu tài khoản
- Các tài khoản đang hoạt động của nhân viên bị sa thải cần phải xóa
- Lỗi cấu hình phần cứng
- Lạm dụng nhiệt độ hoạt động cho phép
- Xóa dữ liệu khỏi các tài nguyên quan trọng
- Sử dụng các tài nguyên của công ty không trong thời gian làm việc
- Máy ảo và xóa ảnh chụp màn hình nhanh
- Kết nối thiết bị mới với cơ sở hạ tầng CNTT
- Thay đổi chính sách nhóm
- Sử dụng TeamViewer, truy cập từ xa vào tài nguyên của công ty
- Các sự kiện quan trọng trong hệ thống bảo vệ
- Lỗi và hỏng hóc hệ thống thông tin

THIẾT LẬP CHÍNH SÁCH BẢO MẬT

Sau khi cài đặt hệ thống, nhân viên bảo mật thông tin có quyền truy cập vào hơn 300 quy tắc - chính sách bảo mật đã được tạo sẵn. Người dùng có thể tùy chỉnh các chính sách hiện có và tạo ra các chính sách của riêng họ, tức là chọn từ danh sách đã tạo trước đó và thêm vào các chính sách của riêng họ (chức năng kết nối người dùng).

- Các hệ điều hành
- Email servers
- Bộ điều khiển tên miền và máy trạm
- DBMS (Hệ thống quản lý cơ sở dữ liệu)
- Máy chủ và máy trạm Linux
- DLP (Hệ thống chống thất thoát dữ liệu)
- File servers (Máy chủ tập tin)
- Môi trường ảo hóa
- Antiviruses
- Tường lửa và thiết bị bảo mật mạng tích hợp
- Giải pháp trên nền tảng ICloud
- Các nguồn nhật ký hệ thống khác

Các quy tắc tương quan chéo có thể được thiết lập để tìm kiếm các sự cố liên quan đến các sự kiện được thu thập từ nhiều nguồn khác nhau.



Màn hình hiển thị sự cố

ƯU ĐIỂM

- Thực hiện nhanh chóng mà không cần cấu hình sơ bộ chuyên sâu, phần mềm có thể bắt đầu hoạt động trong ngày cài đặt
- Tích hợp với các sản phẩm của SearchInform làm tăng mức độ bảo mật thông tin của một công ty và giúp công ty có thể điều tra đầy đủ sự cố và thu thập cơ sở bằng chứng
- Hệ thống dễ sử dụng, một chuyên gia không có kỹ năng CNTT sẽ có thể nhanh chóng làm quen và sử dụng được phần mềm vì nó không yêu cầu kiến thức về ngôn ngữ lập trình để tạo ra các quy tắc tương quan và tương quan chéo
- Yêu cầu thấp đối với phần cứng và phần mềm; giá cả hợp lý ngay cả đối với các doanh nghiệp quy mô nhỏ

SearchInform FileAuditor

Lượng dữ liệu mà một công ty trung bình lưu trữ là rất lớn. Và một trong số các dữ liệu này chứa các thông tin quan trọng, bí mật: dữ liệu cá nhân và tài chính, thông số kỹ thuật, bản vẽ, v.v. Mỗi nhóm dữ liệu nhạy cảm phải được lưu trữ, xử lý và phân phối theo các quy tắc tương ứng.

DỮ LIỆU QUAN TRỌNG LUÔN BỊ ĐE DỌA

SearchInform FileAuditor là một giải pháp DCAP (kiểm tra và bảo vệ dữ liệu) tự động kiểm tra kho thông tin, tìm kiếm các truy cập vi phạm và theo dõi các thay đổi được thực hiện đối với dữ liệu quan trọng.

FileAuditor giải quyết các tác vụ sau:

Phân loại dữ liệu dễ bị tấn công

Phát hiện file dữ liệu có chứa thông tin quan trọng và phân loại file đó: dữ liệu cá nhân, bí mật kinh doanh, số thẻ tín dụng, v.v.

Lưu trữ dữ liệu quan trọng

Tạo bản sao ẩn của các tệp tin quan trọng được tìm thấy trên PC, máy chủ hoặc các thư mục mạng, lưu lịch sử các bản sửa đổi của chúng. Kho lưu trữ dữ liệu bí mật giúp điều tra sự cố và đảm bảo khôi phục thông tin bị mất.

Kiểm tra quyền truy cập

Tạo điều kiện thuận lợi cho việc kiểm soát truy cập thông tin bí mật - tự động giám sát các tài nguyên mở, các tệp có sẵn cho một người dùng hoặc nhóm cụ thể, các tài khoản đặc quyền.

Giám sát hoạt động của người dùng

Kiểm tra hoạt động của người dùng trong hệ thống tệp và trình tự thời gian của họ. Các chuyên gia bảo mật luôn cập nhật thông tin về những thay đổi được thực hiện đối với tệp (tạo, chỉnh sửa, di chuyển, xóa, v.v.).

The screenshot displays the SearchInform FileAuditor interface. The top section shows a file browser with columns for File, Size, Creation date, and Date of update. Below this, the 'Operations' section is visible, showing a table of file operations with columns for Date/Time, Extension, Computer, User, From IP, MAC, Size, File name, Old name, Device type, End date, Process, Image name, Operation, Old size, and File hash.

Date/Time	Extension	Computer	User	From IP	MAC	Size	File name	Old name	Device type	End date	Process	Image name	Operation	Old size	File hash
8/23/2019 1:53:54 PM		computer	Reserv-@computer\Reserv-@com	192.168.50.132	00:0C:29:3A:9A:76	81,95 KB	C:\Users\Fire\...	C:\Users\Fire\...	...	8/23/2019 1:53:54 PM	explorer.exe	C:\Windows\...	Moving	81,95 KB	638457299691779
8/23/2019 1:53:50 PM		computer	Reserv-@computer\Reserv-@com	192.168.50.132	00:0C:29:3A:9A:76	81,95 KB	C:\Users\Fire\...	C:\Users\Fire\...	...	8/23/2019 1:53:50 PM	explorer.exe	C:\Windows\...	Moving	81,95 KB	638457299691779
8/23/2019 1:53:50 PM		computer	Reserv-@computer\Reserv-@com	192.168.50.132	00:0C:29:3A:9A:76	81,95 KB	C:\Users\Fire\...	C:\Users\Fire\...	...	8/23/2019 1:53:50 PM	explorer.exe	C:\Windows\...	Change	81,95 KB	638457299691779
8/23/2019 1:40:46 PM		computer	Reserv-@computer\Reserv-@com	192.168.50.132	00:0C:29:3A:9A:76	81,95 KB	C:\Users\Fire\...	C:\Users\Fire\...	...	8/23/2019 1:40:46 PM	chrome.exe	C:\Program\...	Reading	81,95 KB	638457299691779
8/23/2019 11:53:56		computer	Reserv-@computer\Reserv-@com	192.168.50.132	00:0C:29:3A:9A:76	81,95 KB	C:\Users\Fire\...	C:\Users\Fire\...	...	8/23/2019 11:53:56	explorer.exe	C:\Windows\...	Copying	81,95 KB	638457299691779

Kiểm tra tệp chứa thông tin bí mật

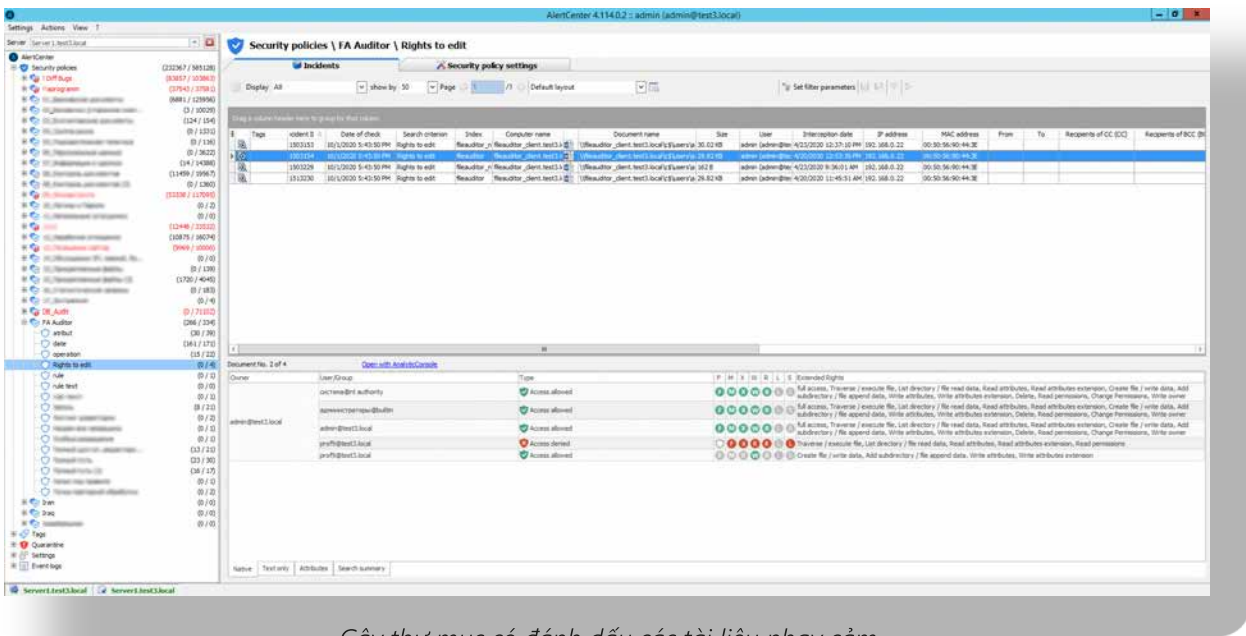
PHÂN TÍCH DỮ LIỆU

Mô-đun phân tích FileAuditor hiển thị kết quả quét hệ thống tệp tin theo các quy tắc đã đặt ra. Trong mục Thiết lập quy tắc (Rule settings) có sẵn các kiểu tìm kiếm khác nhau (theo nội dung, thuộc tính, cụm từ thông dụng, từ điển). Kết quả tìm kiếm có thể được xem dưới dạng báo cáo chi tiết (về nguồn, quyền truy cập, lỗi) hoặc dạng cây.

Chương trình sẽ hiển thị:

- Cây thư mục với dấu hiệu về quyền của người dùng đối với từng thư mục hoặc tệp
- Thao tác trên các tệp quan trọng, ngày tạo và sửa đổi
- Số lượng dữ liệu quan trọng trên đĩa hoặc trong một thư mục
- Đánh dấu tệp (hợp đồng mật, dữ liệu cá nhân, báo cáo tài chính)

Thông báo về các vi phạm chính sách đã đặt ra có thể được thiết lập trong AlertCenter (Trung tâm cảnh báo). Ví dụ: nếu FileAuditor tìm thấy một tài liệu nhạy cảm trên PC của người dùng không có quyền truy cập tài liệu đó, thông báo sẽ tự động được gửi qua email trong thời gian sớm nhất đến người phụ trách về bảo mật.



Cây thư mục có đánh dấu các tài liệu nhạy cảm

Thông tin được thu thập bởi các chương trình và mô-đun quét mạng (network) được ghi vào cơ sở dữ liệu chạy Microsoft SQL Server, và các bản sao của các tệp quan trọng được lưu trữ lại. Đó là cách mà dữ liệu luôn có thể được khôi phục lại ngay cả sau khi đã bị xóa.

ƯU ĐIỂM

- Tích hợp liền mạch giải pháp DCAP (kiểm tra và bảo vệ dữ liệu) vào Rish Monitor (Giám sát rủi ro) làm tăng đáng kể chức năng giảm thiểu rủi ro của hệ thống
- Kiểm soát tải xuống PC và tiết kiệm bộ nhớ - giám sát có thể được lên lịch hoặc kích hoạt bởi một sự kiện hoặc điều kiện cụ thể; chỉ có thể lưu trữ các tài liệu nhạy cảm; một hệ thống chống sao chép sẽ tiết kiệm không gian lưu trữ
- Thiết lập quy tắc có thể tùy chỉnh giúp các chuyên gia tránh khỏi công việc không cần thiết, cho phép họ chỉ tập trung vào việc giám sát các dữ liệu quan trọng
- Các thay đổi thực hiện đối với tệp có thể được theo dõi gần như ngay lập tức - hệ thống lưu một số lượng cụ thể các sửa đổi đối với tệp, giúp ích trong quá trình điều tra nội bộ sau này nếu có sự cố xảy ra

🕒 SearchInform TimeInformer

Đối với một số nhân viên thì khi đi làm họ không tự giác tuân thủ các quy định của công ty, thực hiện các nghĩa vụ của mình. Sẽ luôn có những nhân viên thiếu trách nhiệm, làm việc chểnh mảng, thường xuyên ra ngoài hút thuốc và uống cà phê, tán gẫu với đồng nghiệp, dành thời gian trên các trang mạng xã hội trong giờ làm việc, đi làm muộn nhưng lại hay về sớm.

HOẠT ĐỘNG NHÓM

TimeInformer là giải pháp giám sát nhân viên, bảo vệ doanh nghiệp, công ty khỏi tình trạng làm việc kém hiệu quả và giảm thiểu các tổn thất tài chính liên quan đến nhân sự.

TimeInformer sẽ quét các máy tính làm việc và giúp bạn xác định:



Người vi phạm quy định nơi làm việc, ai hay đến muộn, về sớm, thường xuyên nghỉ giữa giờ



Những người làm công việc phụ khác trong giờ được công ty trả lương



Những người nhàn rỗi, hay ngồi buôn chuyện online, mua sắm trực tuyến, chơi game, hoặc làm các hoạt động không liên quan đến công việc



Những nhân viên bất mãn với công việc và rủ rê đồng nghiệp chống đối lại cấp trên, hoặc những nhân viên trong tình trạng mệt mỏi do khối lượng công việc quá nhiều hoặc quá nhàm chán

Phần mềm xác định thời gian nhàn rỗi và thời gian làm việc của nhân viên, thu thập dữ liệu về phần mềm mà nhân viên sử dụng trong ngày, ghi lại tất cả các trang web đã truy cập và phân loại chúng - các trang web hện hò, mua sắm trực tuyến, tin tức, chương trình truyền hình, v.v. và đánh giá năng suất thực của nhân viên theo các thông số đã cho.

KIỂM SOÁT TRONG THỜI GIAN THỰC

TimeInformer có thể được sử dụng không chỉ trong chế độ nền mà còn ở các chế độ khác. Chương trình kết nối với màn hình PC, micrô và tái tạo những gì đang xảy ra theo thời gian thực.

TimeInformer có thể phát hoặc ghi lại các cuộc đàm phán quan trọng ở chế độ thời gian thực với các đối tác và khách hàng chính. Giải pháp hiển thị ở chế độ thời gian thực những gì được hiển thị trên màn hình của nhân viên của bạn tại bất kỳ thời điểm nào, tối đa 16 PC đồng thời.

TimeInformer có thể được triển khai trên đám mây, cung cấp cho bạn giải pháp mà không cần mua và bảo trì phần cứng.

HỖ TRỢ TRONG QUYẾT ĐỊNH QUẢN LÝ

33 báo cáo được thiết lập trước trong TimeInformer giúp bạn có thể bắt đầu ngay công việc quản lý, cho phép phát hiện nhanh chóng những nhân viên lười biếng, giúp tối ưu hóa quy trình làm việc, sắp xếp nhân sự và đạt được mục tiêu đề ra của công ty.

TimeInformer có các nhóm báo cáo sau:

- Báo cáo về hoạt động của người dùng trong các ứng dụng và trên các trang web.
- Báo cáo về các chương trình có lịch sử cài đặt và xóa phần mềm.
- Báo cáo về các thiết bị có dữ liệu về thiết bị được cài đặt trên PC và các thay đổi trong cấu hình của chúng.

Các báo cáo và thông báo được tùy chỉnh dễ dàng. Hệ thống sẽ tự động gửi thông báo về các vi phạm.

THÂN THIỆN VỚI NGƯỜI DÙNG

Giao diện web sẽ cho phép kiểm soát nhân viên từ mọi nơi trên thế giới. Quyền xem báo cáo và các tùy chọn quản trị được phân biệt theo nhiệm vụ và công việc. Cảnh báo tự động về hoạt động đáng ngờ của nhân viên có thể nhận được qua e-mail.

No.	User	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5		
1	admin																																					
2	Nguyen Van A				9:34	12:12	14:52	10:25		10:41	17:51		10:55		11:43	16:17	11:01		8:09							14:31				15:55	9:22							
3	Nguyen Van B				16:55	14:31	15:07	13:13		17:54	18:15		13:46		18:12	17:25	11:11		17:35										15:33		18:40	17:07						
4	Nguyen Van C				7:21	1:18	0:15	2:47		6:52	0:25		3:11		5:29	7:04	0:10		7:35							0:39			2:45	7:44								
5	Nguyen Van D				9:50	11:49	9:44	10:01	8:59		10:16	11:34	9:25	13:33	11:33		11:11		14:18							9:29	11:25	14:05	11:52	14:33	14:33							
6	Nguyen Van E				17:56	18:04	17:49	16:22	16:34		18:21	17:57	18:11	18:17	18:16		14:51		16:28							6:51	17:20	18:25	15:53	14:33	14:33							
7	Nguyen Van F				7:46	6:15	8:04	6:20	7:35		8:04	5:33	8:45	4:44	7:03		3:39		2:07							0:21	5:55	4:18	4:01	01 c	01 c							

Thời gian biểu trong giao diện web

ƯU ĐIỂM

- Bảo vệ các báo cáo và đưa ra cảnh báo nếu ai đó đang cố tình xóa phần mềm
- Giám sát hoạt động của người dùng ngay cả khi họ làm việc tại nhà hoặc đang đi công tác.
- Giao diện web để truy cập vào kết quả giám sát bên ngoài văn phòng
- Tích hợp với các sản phẩm SearchInform, giúp thực hiện điều tra nội bộ

DỊCH VỤ

SearchInform cung cấp dịch vụ cho các công ty không có bộ phận giảm thiểu rủi ro chuyên dụng hoặc thiếu nguồn lực để tích hợp hệ thống bảo vệ dữ liệu và triển khai giám sát.

Dịch vụ của chúng tôi cho mang lại cho công ty các lợi ích từ việc các giải pháp yêu cầu chi phí tài chính và lao động thấp, không cần thuê chuyên gia. Một khách hàng có được hệ thống cùng với một nhóm các nhà phân tích có nhiều kinh nghiệm trong lĩnh vực này. Các chuyên gia bắt đầu làm việc ngay sau khi triển khai mà không cần đào tạo, không nghỉ phép, không nghỉ ốm.

Tùy chọn dưới dạng dịch vụ luôn có sẵn cho mọi sản phẩm của SearchInform. Một trong số chúng có thể được triển khai trên đám mây giúp tiết kiệm tài chính của công ty vì không cần phải mua phần cứng và chi phí bảo trì.

Sản phẩm	Như 1 dịch vụ	Mô hình triển khai trên đám mây
SearchInform DLP	+	+
SearchInform Risk Monitor	+	+
SearchInform SIEM	+	-
SearchInform FileAuditor	+	+
SearchInform TimeInformer	+	+
SearchInform ProfileCenter	+	+

NGUYÊN TẮC LÀM VIỆC



Chuyên gia thiết lập hệ thống phù hợp với các yêu cầu do khách hàng đặt ra.



Khách hàng được bàn giao hoàn toàn để làm việc với hệ thống.



Sau khi sự cố được phát hiện chuyên gia sẽ liên hệ với khách hàng (phương tiện liên lạc được chọn trước).



Chuyên gia cung cấp cho khách hàng các báo cáo sự cố trong một khung thời gian nhất định (một lần một ngày / tuần / tháng).



Khách hàng có thể làm việc với hệ thống đồng thời cùng với chuyên gia hoặc độc lập.



Khách hàng có thể giao nhiệm vụ, hoặc yêu cầu cho các chuyên gia.

BÀI TOÁN - GIẢI PHÁP

Dịch vụ của chúng tôi cho phép phát hiện những điểm yếu trong công ty trong một khoảng thời gian ngắn (kết quả đầu tiên nhận được trong vòng 1-3 tháng).

Các chuyên gia làm việc với khách hàng, sẽ giám sát việc triển khai giải pháp và đưa ra quyết định dựa trên kết quả của các báo cáo và điều tra sự cố.

Summary report on the incidents. Details on each incident are available 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 CY to USB drive.	It is not clear why the employee copied some strange	Link
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, employee 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	Edtion 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 correspondence 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 agreement.	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 jobs.	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 accounts to another employee.	Possibly wants to find employment for family.	Link
22		Employee name	Chatting on social network, telling about some acquaintance drug addict from Poland who has reason. 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	Top 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

Báo cáo tóm tắt về sự cố

ƯU ĐIỂM

- Thái độ khách quan và cách tiếp cận chuyên nghiệp - đội ngũ phân tích cung cấp dịch vụ của chúng tôi không có quan hệ trực tiếp các nhân viên, do đó, yếu tố con người (yếu tố chủ quan) trong quá trình điều tra bị loại trừ.
- Chia sẻ kinh nghiệm và kiến thức về công ty với hơn 3000 khách hàng. Đội ngũ của chúng tôi sẽ có thể tinh chỉnh phần mềm sao cho phù hợp môi trường hoạt động đặc thù của một công ty, tổ chức giúp cho công ty, tổ chức đó thu được lợi ích tối đa từ các chức năng của hệ thống.

LIÊN HỆ

ARGENTINA

Buenos Aires

Phone: +54 0 11 5984 2618

+54 9 11 5158 8557

Email: r.martinez@searchinform.com

BRAZIL

Sao Paulo

Phone: +55 11 43 80 19 13

+7925 681 1803

Email: v.prestes@searchinform.com

KAZAKHSTAN

Almaty

Phone: +7 727 239 30 36

+7 727 222 17 95

Email: d.stelchenko@searchinform.ru

TRUNG ĐÔNG-BẮC PHI

Phone: +375 25 708 77 69

Email: yamen@searchinform.com

London

Phone: +44 0 20 3808 4340

Email: uk@searchinform.com

SERBIA

Belgrade

Phone: +381 11 45 323 10

+381 69 44 210 44

Email: m.prerad@searchinform.com

NAM PHI

Centurion

Phone: +27 12 683 8816

Email: jorina@searchinform.com
