SEARCHINFORM

NỀN TẢNG GIẢM THIỂU RỦI RO NỘI BỘ

vn.searchinform.com

1995 Công ty được thành lập

3 000 000+
máy tính được bảo vệ bởi phần mềm của SearchInform

4 000+ Khách hàng trên toàn thế giới

6 sản phẩm cung cấp khả năng bảo vệ dữ liệu toàn diện trước các mối đe dọa

2017

Phần mềm SearchInform được đưa vào
Gartner Magic Quadrant

2019
SearchInform bắt đầu cung cấp Dịch vụ giám sát

2020
Các giải pháp đám mây của SearchInform được công bố

The Radicati Group
đã đưa SearchInform vào
nghiên cứu Enterprise Data Loss Prevention Market giai đoạn 2017–2021

2018-2020

Chuỗi sự kiện
Road Show SearchInform được tổ chức tại
Mỹ Latinh, Trung Đông, Bắc Phi, Nam Phi, Ấn Độ và Indonesia

2022-2023
+9 quốc gia Bắc Phi — SearchInform mở rộng sự hiện diện tại khu vực

2023
SearchInform mở văn phòng tập trung vào dịch vụ tại
Dubai (UAE)

2010
Trung tâm đào tạo
được thành lập

16 Khóa đào tạo nâng cao dành cho chuyên gia an ninh thông tin

2 Khóa đào tạo an ninh mạng dành cho người dùng

SẢN PHẨM VÀ DỊCH VỤ

SearchInform FileAuditor
Trang 4-7

SearchInform DLP
Trang 8-9

SearchInform Risk Monitor
Trang 10-18

SearchInform TimeInformer
Trang 19-20

SearchInform Managed Security Services
Trang 21-25

Giải pháp tích hợp của SearchInform
Trang 26-28

SearchInform SIEM
Trang 29-31

SearchInform FileAuditor

Lượng dữ liệu mà một doanh nghiệp thông thường lưu trữ là rất lớn, và một phần trong đó chứa các thông tin mật như dữ liệu cá nhân, dữ liệu tài chính, bản vẽ kỹ thuật và nhiều loại dữ liệu khác. Mỗi nhóm dữ liệu nhạy cảm phải được lưu trữ, xử lý và chia sẻ theo đúng các quy định liên quan.

- DỮ LIỆU QUAN TRỌNG LUÔN SẴN SÀNG TRONG TẦM TAY
- BẢO VỆ TỆP TRONG MỌI ỨNG DỤNG

Nền tảng SearchInform cung cấp CƠ CHẾ BẢO VỆ ĐA TẦNG toàn diện trước các mối đe dọa an toàn thông tin.

CÁC CẤP ĐỘ BẢO MẬT THÔNG TIN được bao phủ bởi các sản phẩm của SearchInform:

CẤP ĐỘ THỨ NHẤT	CẤP ĐỘ THỨ HAI	CẤP ĐỘ THỨ BA
Bảo vệ hệ thống tệp, được triển khai với sự hỗ trợ của FileAuditor (công cụ DCAP).	Hệ thống DLP đảm bảo bảo vệ ở cấp độ máy trạm, các kênh dữ liệu và các rủi ro liên quan đến yếu tố con người.	Risk Monitor cung cấp giải pháp toàn diện cho việc quản lý rủi ro và bảo vệ dữ liệu.

Các hệ thống được tích hợp liền mạch, hoạt động trên một nền tảng công nghệ thống nhất và có thể được triển khai chỉ trong vài giờ.

DỮ LIỆU QUAN TRỌNG LUÔN TRONG TẦM KIỂM SOÁT

SearchInform FileAuditor là giải pháp DCAP (Data-Centric Audit and Protection) được thiết kế để kiểm toán tự động các hệ thống lưu trữ thông tin. Hệ thống giúp phát hiện các vi phạm quyền truy cập và theo dõi các thay đổi đối với dữ liệu quan trọng.

Dưới đây là cách FileAuditor giải quyết bài toán giám sát an ninh đối với dữ liệu quan trọng:

Phân loại dữ liệu nhạy cảm

Phát hiện các tệp trong luồng tài liệu có chứa thông tin quan trọng và gắn nhãn đặc biệt cho từng tệp, cho biết loại thông tin mà tệp đó chứa, chẳng hạn như: dữ liệu cá nhân, bí mật thương mại, số thẻ tín dụng, v.v.

Kiểm toán quyền truy cập

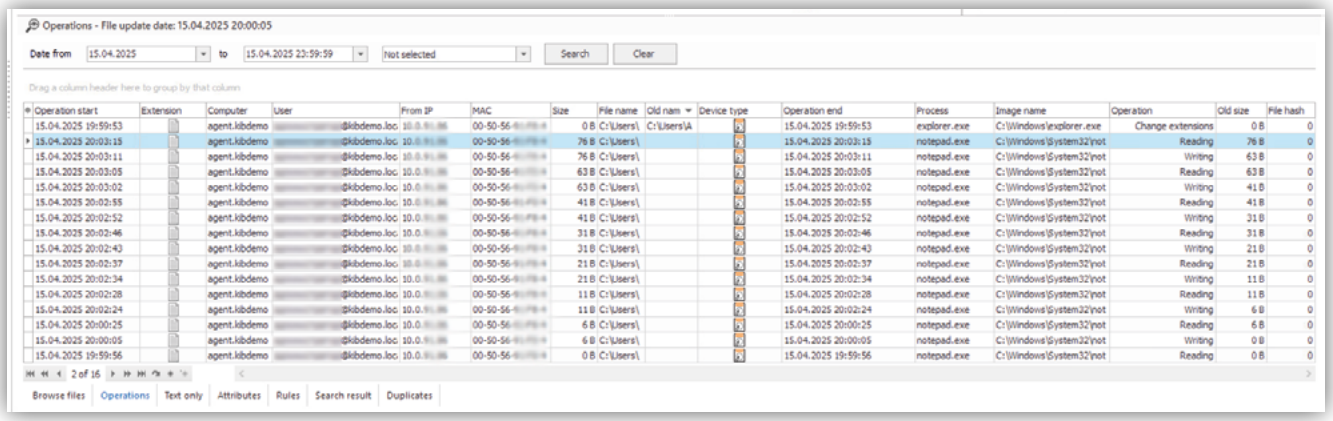
Kiểm soát quyền truy cập vào dữ liệu (toàn quyền, chỉnh sửa, ghi, đọc, v.v.). Theo dõi các nhân viên có quyền truy cập trái phép vào dữ liệu. Phát hiện các tệp chứa thông tin mật được lưu trữ vi phạm các quy định bảo mật đã thiết lập (trong các khu vực công khai, thư mục mạng chia sẻ, máy tính của nhân viên, v.v.).

Lưu trữ tài liệu quan trọng

Tạo các bản sao dự phòng (shadow copy) của các tệp quan trọng được tìm thấy trên máy tính, máy chủ hoặc trong các thư mục mạng, đồng thời ghi lại lịch sử các thay đổi đối với chúng. Kho lưu trữ dữ liệu mật hỗ trợ điều tra sự cố và đảm bảo khả năng khôi phục thông tin bị mất.

Giám sát và chặn các hành động của người dùng

Kiểm toán các thao tác của người dùng đối với hệ thống tệp. Bộ phận an toàn thông tin CNTT luôn nắm được thông tin cập nhật về vòng đời của tệp (tạo, chỉnh sửa, truyền tải, xóa, v.v.). Hệ thống có thể chặn quyền truy cập vào tệp và ngăn chặn việc truyền tệp thông qua bất kỳ ứng dụng nào.



Chế độ hoạt động: giám sát hoạt động của tệp

SEARCHINFORM FILEAUDITOR HOẠT ĐỘNG NHƯ THẾ NÀO?

Thông tin thu thập được sẽ được lưu trữ trong cơ sở dữ liệu; các tài liệu quan trọng vẫn có thể truy cập được ngay cả khi chúng đã bị xóa khỏi máy tính của người dùng.

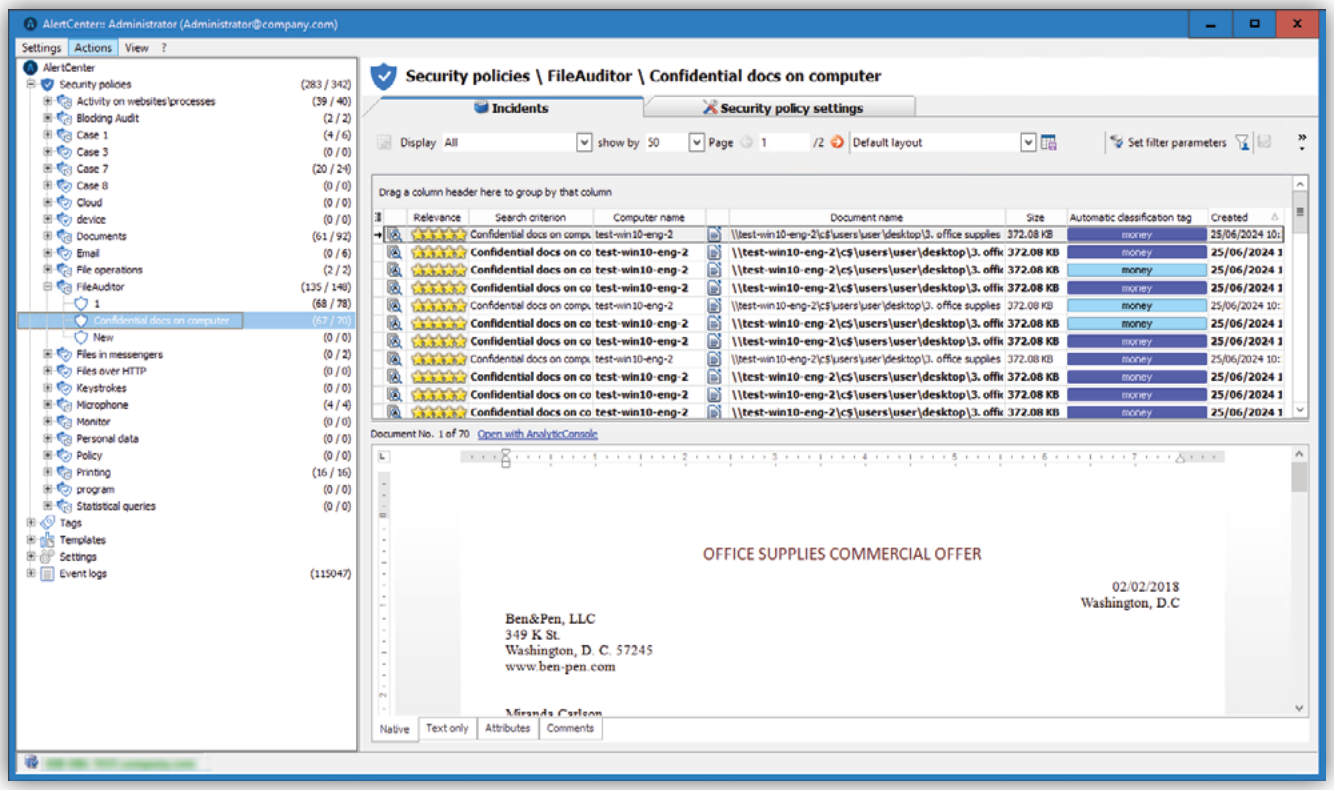
PHÂN TÍCH DỮ LIỆU

Mô-đun phân tích của FileAuditor trực quan hóa kết quả quét hệ thống tệp dựa trên các quy tắc được thiết lập sẵn. Các thiết lập quy tắc hỗ trợ nhiều loại tìm kiếm khác nhau. Kết quả có thể được hiển thị dưới dạng các báo cáo trực quan (ví dụ: nguồn dữ liệu, quyền truy cập, lỗi) hoặc dưới dạng cấu trúc cây.

Hệ thống hiển thị:

- Cấu trúc cây thư mục thể hiện quyền truy cập của người dùng đối với từng thư mục hoặc tệp
- Các thao tác đối với các tệp quan trọng, bao gồm thời điểm tạo và chỉnh sửa
- Số lượng tài liệu quan trọng trên một ổ đĩa hoặc trong một thư mục
- Nhãn phân loại tệp, ví dụ: NDA, dữ liệu cá nhân, báo cáo tài chính

Thông báo vi phạm chính sách có thể được cấu hình trong AlertCenter. Ví dụ, nếu FileAuditor phát hiện một tệp nhạy cảm trên máy tính của người dùng mà không có quyền truy cập phù hợp, cán bộ phụ trách quản lý rủi ro sẽ tự động nhận được thông báo qua email.



AlertCenter

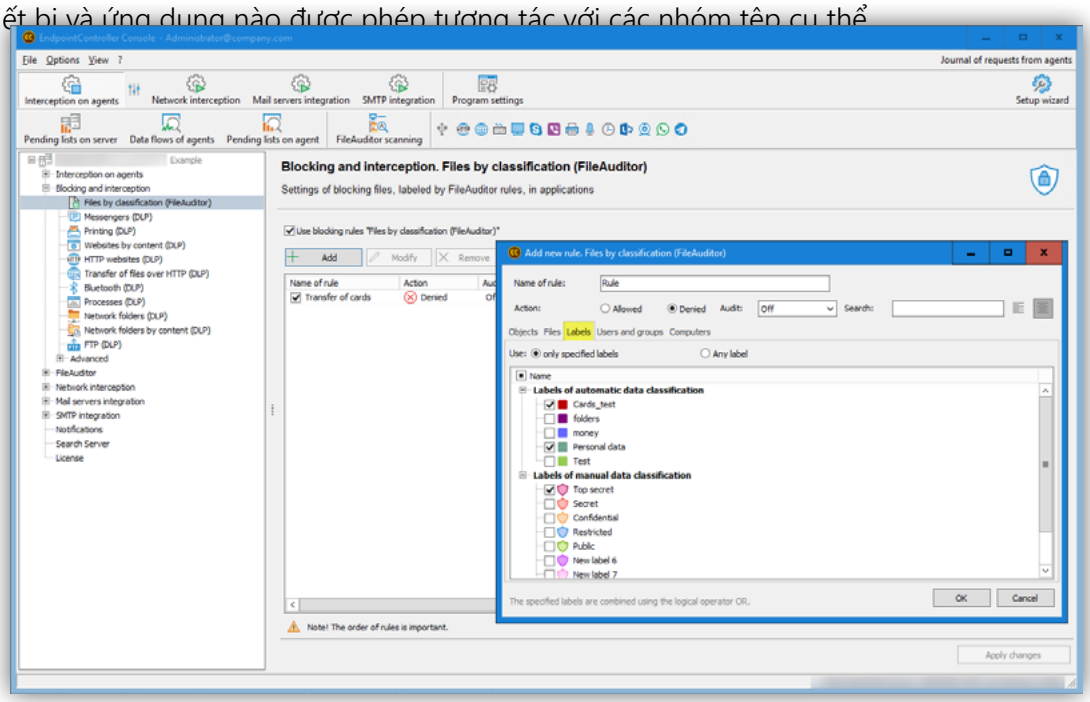
Thông tin được thu thập bởi các agent và mô-đun quét mạng được lưu trữ trong cơ sở dữ liệu chạy trên Microsoft SQL Server hoặc PostgreSQL, trong khi các bản sao của các tệp quan trọng được lưu giữ trong kho lưu trữ. Điều này đảm bảo rằng các tài liệu vẫn có thể truy cập được ngay cả sau khi đã bị xóa.

BẢO VỆ DỮ LIỆU

Cơ chế chặn dựa trên nội dung giúp ngăn chặn các thao tác đối với tệp quan trọng, bao gồm các hành động trái phép đối với tài liệu trong nhiều ứng dụng khác nhau, các hoạt động truyền tải đáng ngờ hoặc truy cập bởi người dùng không được ủy quyền.

Các quy tắc chặn được áp dụng cho cả các tệp được gắn nhãn tự động và các tệp được phân loại thủ công. Hệ thống gán nhãn dựa trên loại thông tin, chẳng hạn như bí mật thương mại, thông tin cá nhân hoặc hợp đồng.

Các quyền và hạn chế truy cập được cấu hình dựa trên phân loại thông tin, xác định những người dùng, thiết bị và ứng dụng nào được phép tương tác với các nhóm tệp cụ thể.



Cấu hình các quy tắc chặn theo nhãn trong SearchInform FileAuditor

FileAuditor cho phép chặn truy cập vào tệp thông qua bất kỳ ứng dụng nào, bất kể phiên bản, loại hay nguồn gốc của ứng dụng. Các hạn chế được thực thi ở cấp độ hệ thống tệp, nơi hệ thống kiểm soát việc ứng dụng có được phép hay bị từ chối quyền đọc dữ liệu. Điều này cho phép kiểm soát việc đọc, chỉnh sửa và chuyển tiếp các tài liệu chứa thông tin mật, đồng thời cho phép cấu hình các thiết lập truy cập tệp khác.

ƯU ĐIỂM

- Tích hợp liền mạch giải pháp DCAP vào chức năng của hệ thống DLP.
- Kiểm soát tải của máy tính và tiết kiệm bộ nhớ — việc giám sát có thể được lên lịch hoặc kích hoạt theo các sự kiện hay điều kiện cụ thể; hệ thống có thể chỉ lưu trữ các tài liệu nhạy cảm và cơ chế loại bỏ trùng lặp giúp tiết kiệm dung lượng lưu trữ.
- Khả năng triển khai trên nền tảng đám mây — phần mềm có thể được triển khai trên cloud, cho phép các doanh nghiệp không có hạ tầng CNTT riêng vẫn có thể sử dụng hệ thống.
- Thiết lập quy tắc linh hoạt giúp chuyên gia tránh các tác vụ không cần thiết và tập trung vào việc giám sát dữ liệu quan trọng.
- Theo dõi thay đổi tệp theo thời gian thực — hệ thống lưu lại một số phiên bản tệp nhất định để hỗ trợ điều tra nội bộ.
- Bảo vệ tệp chủ động — hệ thống có thể chặn truy cập vào tài liệu để ngăn chặn các chỉnh sửa hoặc truyền tải trái phép.

SearchInform DLP

Bảo vệ doanh nghiệp khỏi các rò rỉ thông tin mật và kiểm soát dữ liệu đang truyền tải (data in motion).

Hệ thống giám sát các kênh truyền dữ liệu phổ biến, phân tích nội dung, phát hiện và ngăn chặn các vi phạm, đồng thời cung cấp báo cáo cho bộ phận phụ trách.

SEARCHINFORM CUNG CẤP GIẢI PHÁP BẢO VỆ TIN CẬY CHO DỮ LIỆU ĐANG TRUYỀN TẢI

Bảo vệ dữ liệu doanh nghiệp của bạn và tận dụng các tính năng sau:

- Kiểm soát các kênh truyền dữ liệu chính được sử dụng trong hoạt động kinh doanh;
- Các công cụ phân tích nâng cao, bao gồm OCR, Similar Content Search và Image Search;
- Lưu trữ chi tiết các sự cố để phục vụ kiểm toán và điều tra toàn diện;
- Các tùy chọn triển khai bao gồm cài đặt tại chỗ (on-premises) hoặc triển khai trên đám mây, với khả năng tích hợp với Microsoft 365.

1. Giám sát các kênh truyền dữ liệu được sử dụng phổ biến trong doanh nghiệp.
2. Kiểm soát các công cụ truy cập từ xa và công cụ hiển thị màn hình.
3. Tự động kiểm tra dữ liệu theo các chính sách bảo mật được cấu hình sẵn.
4. Thông báo cho cán bộ an toàn thông tin và ngăn chặn việc truyền dữ liệu mật khi phát hiện sự cố tiềm ẩn.
5. Cảnh báo các hoạt động đáng ngờ và các bất thường trong mạng.
6. Tạo kho lưu trữ sự cố với nhật ký chi tiết về các hành động của người dùng.

Tuân thủ đầy đủ các yêu cầu pháp lý và quy định

Giải pháp giúp đảm bảo việc tuân thủ được duy trì nhất quán trong toàn bộ tổ chức.

Bảo vệ dữ liệu toàn diện và ngăn ngừa các mối đe dọa

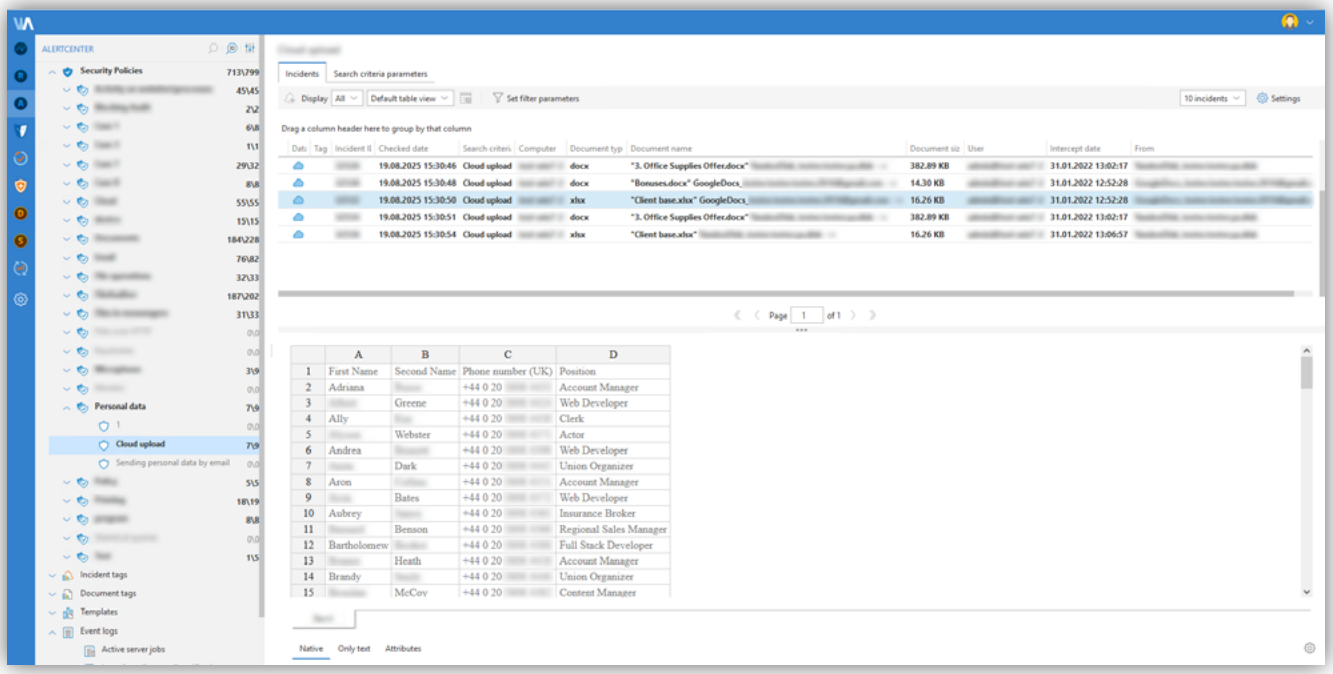
SearchInform DLP phát hiện và phân tích các lỗ hổng trong quá trình truyền dữ liệu, đồng thời sử dụng các công cụ phân tích nâng cao để tương quan và nhận diện các mối đe dọa.

Bảo vệ dữ liệu doanh nghiệp 24/7

Giải pháp bảo vệ thông tin của doanh nghiệp bất kể nhân viên của bạn đang làm việc ở đâu.

CHÍNH SÁCH BẢO MẬT

Hệ thống cung cấp hơn 250 chính sách bảo mật dựng sẵn, bao gồm các chính sách chung và các chính sách dành riêng cho từng ngành. Ngoài ra, người dùng cũng có thể tạo các chính sách bảo mật tùy chỉnh.



Chính sách bảo mật trong AlertCenter

ƯU ĐIỂM

- **Giải pháp có khả năng bảo vệ tốt nhất trên thị trường DLP hiện tại,** cung cấp cơ chế ngăn chặn rò rỉ dữ liệu dựa trên nội dung thông qua tin nhắn và tệp trong các ứng dụng nhắn tin, email, dịch vụ đám mây, truy cập desktop từ xa, duyệt web, in ấn và các thiết bị lưu trữ di động.
- **Hỗ trợ các máy trạm chạy Windows/Linux/Mac,** máy chủ DLP cho Windows và Linux, cơ sở dữ liệu MS SQL Server và PostgreSQL, được tối ưu hóa cho việc lưu trữ và phân tích dữ liệu.
- **Các công nghệ phân tích tiên tiến hàng đầu trên thị trường,** bao gồm các mẫu phân tích truyền thống (hơn 430 mẫu có sẵn theo mặc định), các thuật toán thông minh, học máy và phân tích hành vi.
- **Giải pháp không chỉ có khả năng thực hiện chặn (blocking),** mà còn có thể xử lý dữ liệu như mã hóa, cách ly (quarantine) hoặc trả lại email cho người dùng.
- **DLP cung cấp quyền truy cập vào công nghệ profiling tự động,** cho phép đánh giá các rủi ro liên quan đến yếu tố con người và hỗ trợ đưa ra các quyết định quản lý phù hợp.

SearchInform Risk Monitor

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

Risk Monitor bảo vệ doanh nghiệp khỏi các tổn thất về tài chính và uy tín do các mối đe dọa từ bên trong gây ra.

GIẢI PHÁP SEARCHINFORM TRIỂN KHAI TẠI CHỖ VÀ TRÊN ĐÁM MÂY

Doanh nghiệp không cần phải lựa chọn giữa bảo mật, khả năng sử dụng và chi phí vì giải pháp có thể được triển khai trên nền tảng đám mây. Không cần phần cứng chuyên dụng: Risk Monitor thu thập, xử lý và lưu trữ dữ liệu trong môi trường ảo. Mô hình triển khai này phù hợp với các doanh nghiệp không có hạ tầng CNTT riêng, có văn phòng tại nhiều thành phố và có số lượng lớn nhân viên làm việc từ xa.

NỀN TẢNG QUẢN LÝ RỦI RO TOÀN DIỆN SỬ DỤNG MỘT AGENT DUY NHẤT

Bảo mật lấy người dùng làm trung tâm

- Giúp nâng cao năng suất làm việc của nhân viên
- Bảo vệ doanh nghiệp trước các rủi ro liên quan đến nhân sự và dự đoán các mô hình hành vi của nhân viên
- Hỗ trợ quản lý mức độ gắn kết và trung thành của đội ngũ
- Kiểm soát yếu tố con người

Hỗ trợ tuân thủ

- Giải quyết các yêu cầu tuân thủ quy định
- Thực hiện phân tích pháp chứng số và điều tra hồi cứu

Bảo mật lấy dữ liệu làm trung tâm

- Giảm thiểu rủi ro rò rỉ dữ liệu
- Bảo vệ các dữ liệu nhạy cảm nhất trên các thiết bị của doanh nghiệp

GIẢI PHÁP MỞ RỘNG

- Phát hiện các sự cố nội bộ có chủ đích liên quan đến gian lận và trục lợi trong doanh nghiệp
- Hỗ trợ tuân thủ các quy định pháp lý và hỗ trợ quá trình điều tra
- Kiểm soát yếu tố con người và dự đoán các rủi ro liên quan đến nhân sự
- Hoạt động như một hệ thống cảnh báo sớm, phát hiện các mối đe dọa tiềm ẩn hoặc các điều kiện có thể dẫn đến vi phạm và cảnh báo về các rủi ro có thể xảy ra

Risk Monitor cung cấp bộ công cụ mạnh mẽ và tự động hóa để giám sát nhân viên, đánh giá rủi ro và thực hiện kiểm toán nội bộ. Giải pháp đảm bảo rằng các chính sách của doanh nghiệp tuân thủ các quy định liên quan và giúp đánh giá mức độ phù hợp của các biện pháp bảo mật với các tiêu chuẩn mới nhất của ngành.

Giải pháp được xây dựng dựa trên khung quản lý rủi ro, giúp phát hiện gian lận trong doanh nghiệp và ngăn ngừa các tổn thất tài chính.

KHẢ NĂNG

Thu thập thông tin chi tiết về các hoạt động của người dùng để tái dựng từng bước một vụ vi phạm

Bảo vệ doanh nghiệp trước các rủi ro liên quan đến nhân sự và dự đoán các mô hình hành vi của nhân viên

Tạo kho lưu trữ các thông tin bị chặn hoặc thu thập được, giúp hỗ trợ tuân thủ quy định và tăng cường các chính sách bảo mật nhằm giảm thiểu rủi ro

Giúp nâng cao năng suất làm việc của nhân viên và hỗ trợ quản lý mức độ gắn kết của đội ngũ

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

THU THẬP DỮ LIỆU

Giải pháp SearchInform đảm bảo bảo vệ tất cả các kênh dữ liệu được sử dụng phổ biến.

E-mail

Thu thập, phân loại và cách ly email. Bảo vệ email doanh nghiệp và email công cộng (Gmail, v.v.). Hỗ trợ kiểm soát email thông qua các giao thức chuẩn của ứng dụng email (IMAP, MAPI, SMTP) cũng như email truy cập qua trình duyệt.

Monitor+Keylogger

Chụp ảnh màn hình và ghi lại hoạt động trên màn hình của người dùng, bao gồm hoạt động của phần mềm. Có thể chụp ảnh hoặc quay video qua webcam, ghi lại thao tác bàn phím, phát hiện các nỗ lực chụp ảnh màn hình bằng thiết bị bên ngoài và hỗ trợ nhận diện sinh trắc học người dùng thông qua nhận diện khuôn mặt.

IM (Instant Messaging)

Thu thập, phân loại và chặn tin nhắn, cuộc gọi và tệp được truyền qua các nền tảng nhắn tin doanh nghiệp và công cộng, bao gồm WhatsApp và Telegram.

Thiết bị kết nối

Thu thập, phân loại, chặn và áp dụng mã hóa bắt buộc đối với các tệp được truyền qua các cổng vào/ra của thiết bị lưu trữ dữ liệu.

Phần mềm

Theo dõi thời gian sử dụng các ứng dụng và trình duyệt, đánh giá năng suất làm việc và phân tích hoạt động của người dùng trong quá trình điều tra nội bộ.

Dịch vụ đám mây

Thu thập, phân loại và chặn các tệp được truyền tới các dịch vụ đám mây hoặc phần mềm cộng tác (ví dụ: Zoom).

Microphone

Âm thanh được tự động chuyển thành văn bản và phân tích bởi hệ thống để phát hiện các vi phạm tiềm ẩn đối với chính sách bảo mật.

HTTP

Thu thập, phân loại và chặn mọi lưu lượng truy cập trình duyệt không được các bộ kiểm soát khác ghi nhận.

FTP

Thu thập, phân loại và chặn lưu lượng FTP.

In ấn

Thu thập, phân loại và chặn các tệp được gửi đi để in.

TRUNG TÂM ĐIỀU KHIỂN

DataCenter

Quản lý các chỉ mục và cơ sở dữ liệu của hệ thống, giám sát trạng thái hoạt động và đảm bảo kết nối với các hệ thống bên thứ ba như Active Directory, SOC và máy chủ thư gửi đi. Quyền truy cập của người dùng được quản lý từ DataCenter.

AlertCenter

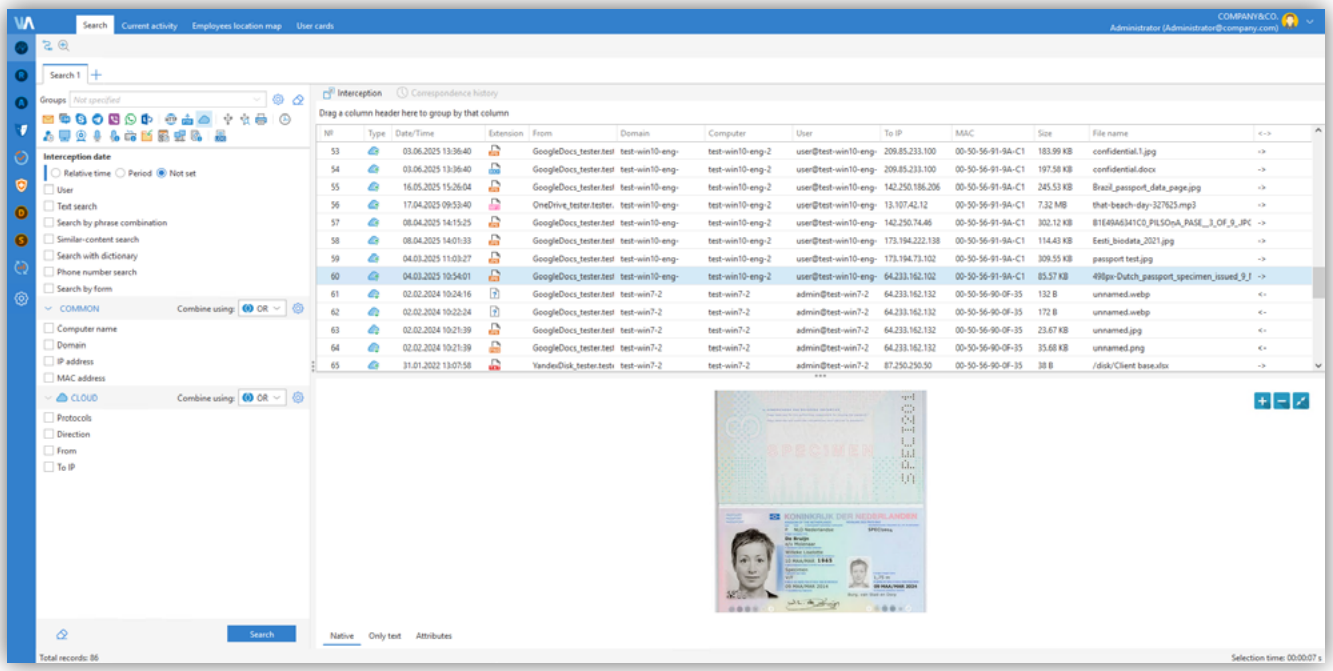
Đây là "trung tâm điều phối" của hệ thống, nơi các chính sách bảo mật được thiết lập. Hệ thống bao gồm hơn 250 chính sách bảo mật được cấu hình sẵn có thể chỉnh sửa. Giải pháp cho phép tạo các chính sách tùy chỉnh để kiểm tra và chặn dữ liệu thu thập được, cấu hình lịch kiểm tra và gửi thông báo.

Các chuyên gia an toàn thông tin có thể xem báo cáo sự cố trong bảng điều khiển AlertCenter trên máy trạm của mình hoặc thông qua giao diện web có thể truy cập từ máy tính xách tay, máy tính bảng hoặc điện thoại thông minh.

AnalyticConsole

AnalyticConsole được sử dụng để phân tích dữ liệu thu thập được và giám sát hoạt động của người dùng. Công cụ cung cấp nhiều thuật toán tìm kiếm và các mẫu báo cáo dựng sẵn để các chuyên gia sử dụng.

Tất cả các chức năng của AlertCenter và AnalyticConsole đều có thể truy cập thông qua giao diện web. Nhờ đó, các chuyên gia bảo mật có thể nhanh chóng phản ứng với các cảnh báo và thực hiện các biện pháp kịp thời đối với các mối đe dọa tiềm ẩn.



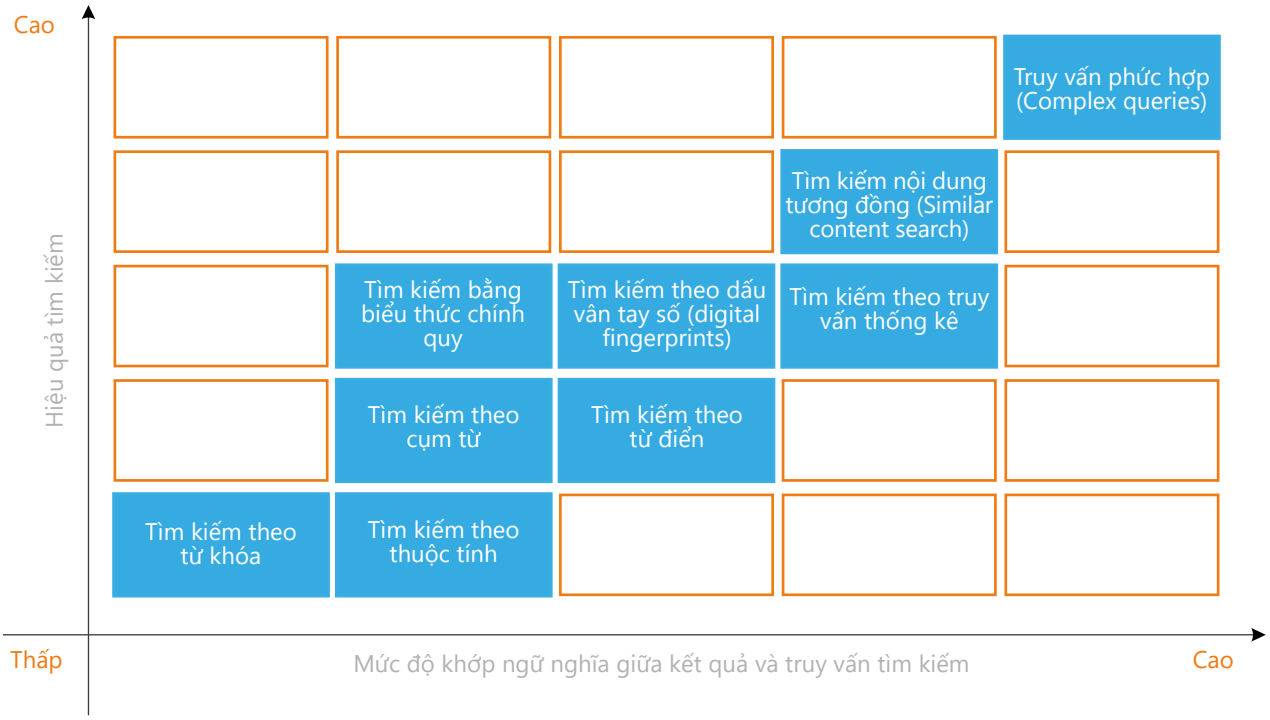
Mô-đun tìm kiếm trong bảng điều khiển web của SearchInform Risk Monitor

KHẢ NĂNG PHÂN TÍCH

Để nâng cao hiệu quả công việc, các chuyên gia an toàn thông tin cần khả năng kiểm soát toàn diện trên tất cả các kênh truyền thông, cũng như các chức năng nâng cao để tìm kiếm và phân tích dữ liệu thu thập được. Mô-đun phân tích mạnh mẽ, nhiều tùy chọn tìm kiếm cùng với phân tích tự động đối với nội dung đồ họa và âm thanh cho phép chỉ một chuyên gia có thể giám sát hoạt động của hàng nghìn nhân viên.

Phân tích văn bản

Các công nghệ tìm kiếm tiên tiến như Similar Content Search và Complex Queries cho phép phân tích chuyên sâu các tin nhắn văn bản và tài liệu. Ví dụ, thuật toán Similar Content Search có thể phát hiện các tài liệu mật ngay cả khi chúng đã bị chỉnh sửa. Thuật toán này tìm kiếm các tệp có nội dung tương đồng về mặt ngữ nghĩa với truy vấn, thay vì chỉ khớp kỹ thuật đơn thuần. Các truy vấn phức hợp kết hợp nhiều thuật toán tìm kiếm, liên kết các truy vấn đơn giản bằng các toán tử logic như AND, OR và NOT.



Phân tích nội dung hình ảnh

Hệ thống xác định các loại hình ảnh được lưu chuyển trong doanh nghiệp như tệp PDF, ảnh hoặc bản quét, và phân loại các tệp hình ảnh tương ứng. Bộ phân loại nội bộ nhận diện các tài liệu phù hợp với các mẫu định sẵn như hộ chiếu, thẻ ngân hàng, giấy phép lái xe, v.v. Công nghệ này cho phép hệ thống phát hiện dữ liệu cá nhân, dữ liệu tài chính và các loại dữ liệu nhạy cảm khác trong kho lưu trữ, ngay cả khi chúng được truyền dưới dạng tài liệu quét.

Phân tích âm thanh

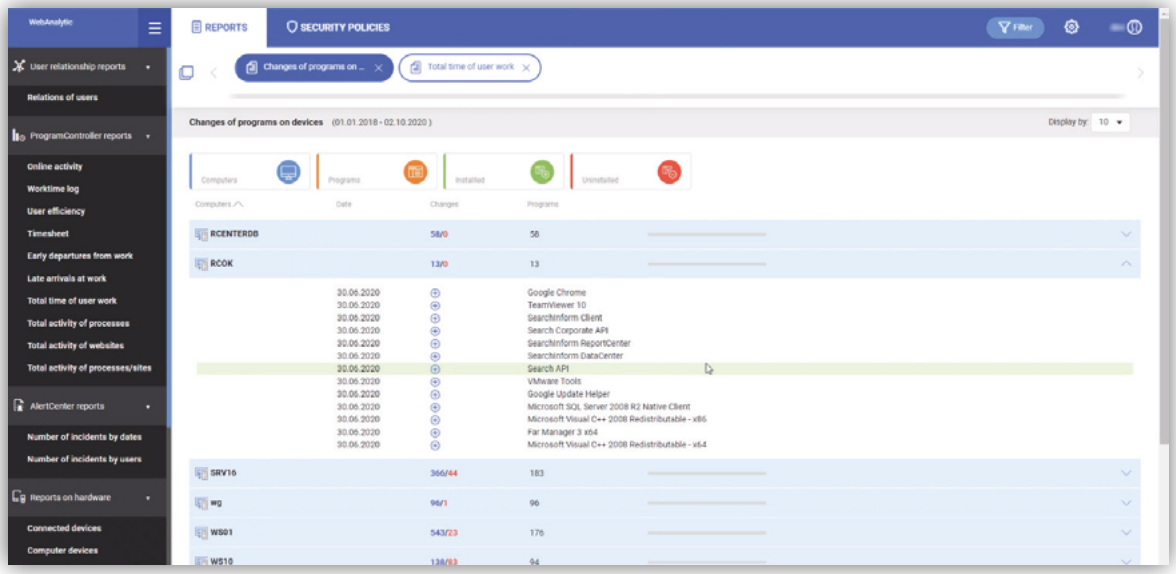
Giải pháp SearchInform chuyển đổi các bản ghi âm thành văn bản và kiểm tra xem bản ghi có tuân thủ các chính sách bảo mật hay không. Hệ thống cũng có tùy chọn tự động bật ghi âm khi phát hiện giọng nói hoặc khi các tiến trình hay chương trình nhất định - được cấu hình trong hệ thống - được khởi chạy.

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

Risk Monitor trực quan hóa tất cả các sự kiện và kết nối trong doanh nghiệp dưới dạng báo cáo, có thể truy cập thông qua AnalyticConsole và giao diện web. Theo mặc định, hệ thống cung cấp hơn 30 mẫu báo cáo tiêu chuẩn. Trình tạo báo cáo cho phép tạo các báo cáo tùy chỉnh mà không bị giới hạn về tiêu chí.

Báo cáo phần mềm và phần cứng

Giải pháp ghi nhận mọi thay đổi đối với phần cứng đã cài đặt và các thiết bị được kết nối, hỗ trợ quản lý tài sản và ngăn chặn tình trạng mất cắp hoặc thay thế thiết bị trái phép. Risk Monitor cũng báo cáo các hoạt động cài đặt và gỡ cài đặt phần mềm.

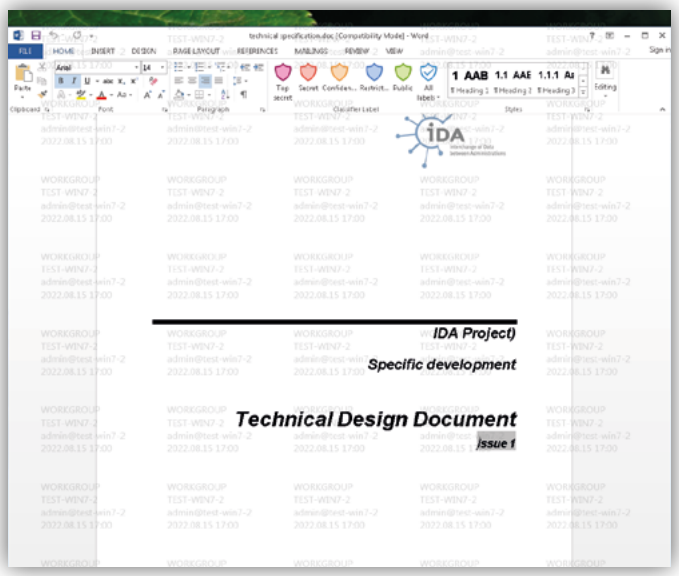


Báo cáo phần mềm và phần cứng

ĐIỀU TRA VÀ KIỂM SOÁT

Phát hiện rò rỉ khi dữ liệu bị trích xuất thông qua ảnh chụp màn hình hoặc ảnh chụp màn hình máy tính

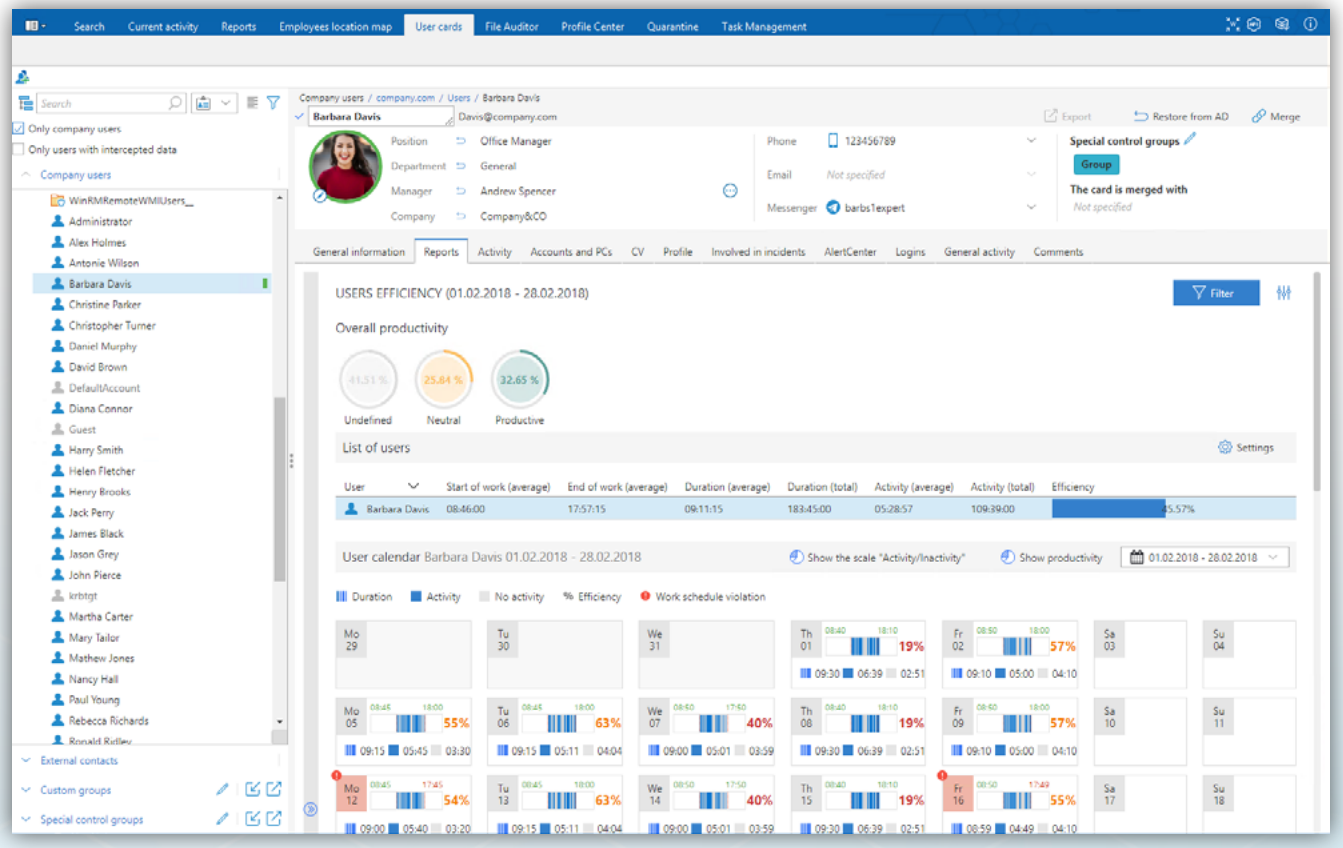
Việc xác định nguồn rò rỉ khi người dùng chụp ảnh màn hình hoặc chụp ảnh màn hình máy tính là rất khó. Công cụ watermark của SearchInform Risk Monitor giải quyết vấn đề này. Bằng cách phân tích ảnh chụp màn hình hoặc ảnh chụp màn hình của một máy trạm được bảo vệ được tìm thấy từ nguồn bên ngoài, chuyên gia an toàn thông tin có thể dễ dàng xác định nguồn gốc của việc rò rỉ dữ liệu thông qua các watermark hiển thị. Watermark chứa thông tin về máy tính và nhân viên đang sử dụng máy đó.



Watermark được chèn bởi SearchInform Risk Monitor

Hồ sơ người dùng

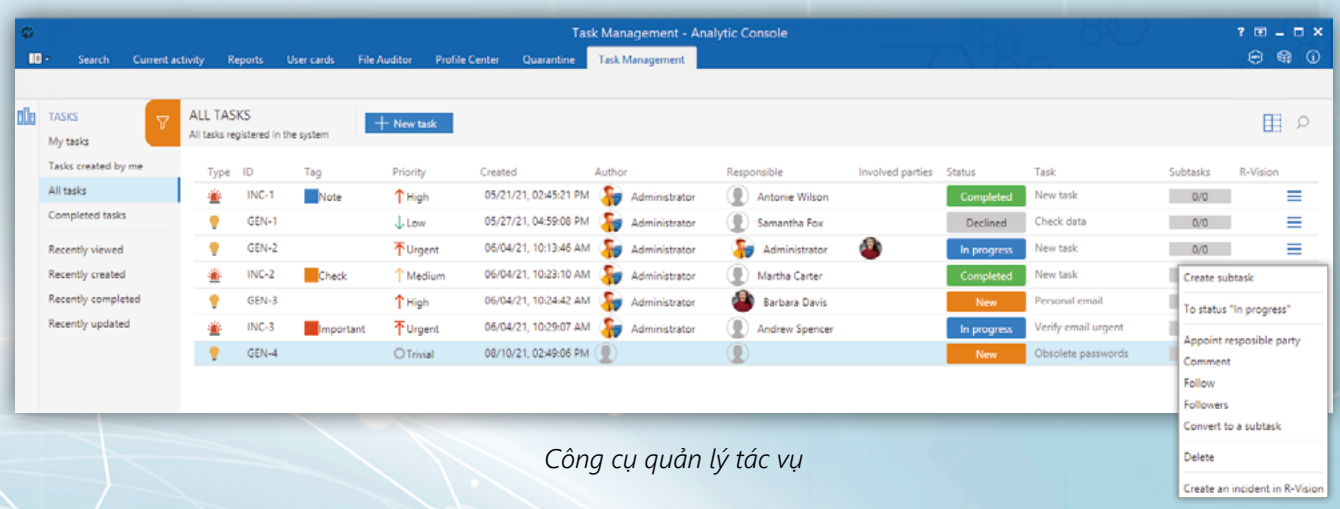
User Card tập hợp một "hồ sơ" cho từng nhân viên, tự động bao gồm tất cả các sự cố mà họ có liên quan. User Card chứa các báo cáo cá nhân, thông tin cá nhân của nhân viên, lịch sử công việc và các thông tin liên quan khác.



Hồ sơ người dùng

Quản lý điều tra

Task Manager giúp các chuyên gia an toàn thông tin phối hợp và quản lý các nhiệm vụ liên quan đến bảo mật. Công cụ này cho phép phân công nhiệm vụ, theo dõi tiến độ điều tra và tạo báo cáo kết quả, bao gồm việc chuyển các báo cáo này đến SOC (Security Operations Center).



Công cụ quản lý tác vụ

ĐẶC ĐIỂM ĐỘC ĐÁO

1

Các tính năng phân tích độc đáo không có trong các công cụ khác

Risk Monitor cung cấp nhiều tính năng phân tích, bao gồm các công cụ phổ biến như tìm kiếm theo từ điển, biểu thức chính quy và dấu vân tay số (digital fingerprints). Ngoài ra, hệ thống còn hỗ trợ các tính năng nâng cao như tìm kiếm hình ảnh tương tự, truy cập các bản ghi âm bằng công nghệ chuyển giọng nói thành văn bản (speech-to-text) và phân tích nội dung trong các bản ghi video về hoạt động của người dùng.

2

Công cụ điều tra chất lượng cao trong một giải pháp

Risk Monitor ghi lại âm thanh các cuộc trao đổi của nhân viên và video về các hành động của họ. Giải pháp ghi nhật ký mọi thao tác của người dùng đối với tệp và thư mục, đồng thời kiểm tra nhật ký hệ thống, thiết bị và phần mềm. Hệ thống cũng giám sát các hành vi vi phạm thông qua các kênh âm thanh và video theo thời gian thực.

3

Kiểm soát hiệu suất làm việc của người dùng

SearchInform Risk Monitor tự động đánh giá hiệu quả làm việc của người dùng trong các ứng dụng và trên các trang web. Chức năng này giúp tăng cường kỷ luật trong doanh nghiệp và phát hiện các vấn đề trong quy trình kinh doanh.

4

Độ ổn định của hệ thống đã được kiểm chứng dưới tải cao

SearchInform được nhiều doanh nghiệp quy mô lớn trong các ngành khác nhau tin tưởng, chứng minh khả năng hoạt động ổn định của hệ thống ngay cả trong điều kiện tải cao và trong các môi trường CNTT đa dạng.

5

Mở rộng tính năng thông qua hệ sinh thái sản phẩm thống nhất

SearchInform cung cấp bộ giải pháp toàn diện bao gồm Risk Monitor, DLP, SIEM và FileAuditor (giải pháp DCAP). Tất cả các hệ thống được xây dựng trên một nền tảng công nghệ thống nhất, cho phép tích hợp liền mạch và triển khai chỉ trong vài giờ.

6

Hỗ trợ đa nền tảng và truy cập từ mọi thiết bị

Giao diện người dùng của SearchInform Risk Monitor có thể được sử dụng theo hai cách: dưới dạng ứng dụng máy khách (client application) trên Windows hoặc dưới dạng phiên bản web.

ƯU ĐIỂM

Mô-đun phân tích mạnh mẽ

Cung cấp các giải pháp nhanh chóng và linh hoạt để cấu hình cảnh báo và phân tích luồng dữ liệu mà không cần thuê chuyên gia bên thứ ba. Với sản phẩm của SearchInform, một chuyên gia có thể giám sát hoạt động của hàng nghìn nhân viên.

Bảo vệ sự cố theo hướng chủ động

Risk Monitor cung cấp cơ chế chặn nội dung thông minh trên tất cả các kênh được kiểm soát nhằm đảm bảo người dùng không thể truyền tệp hoặc tin nhắn chứa nội dung mật. Giao diện agent cũng thông báo cho người dùng về các vi phạm chính sách vô ý, góp phần xây dựng văn hóa an toàn thông tin trong doanh nghiệp.

Kiểm soát truy cập từ xa

Giải pháp SearchInform bảo vệ dữ liệu được truyền qua các môi trường ảo và các công cụ truy cập từ xa. Việc giám sát được thực hiện ở cấp clipboard, trong quá trình kết nối thiết bị lưu trữ ảo, cũng như ở cấp các chức năng phần mềm cụ thể (ví dụ: truyền tệp qua menu ngữ cảnh của TeamViewer).

Bộ phận triển khai và Trung tâm đào tạo

Kinh nghiệm thực tiễn với hơn 4.000 doanh nghiệp thuộc nhiều lĩnh vực khác nhau cho phép chúng tôi nhanh chóng xây dựng các bộ chính sách bảo mật riêng, phù hợp với các nhiệm vụ cụ thể và đặc thù hoạt động của từng khách hàng.

Triển khai dễ dàng mà không cần thay đổi cấu trúc mạng

Các chuyên gia CNTT của khách hàng có thể cài đặt giải pháp SearchInform chỉ trong vài giờ. Quá trình cài đặt không ảnh hưởng đến hoạt động của các hệ thống thông tin nội bộ của doanh nghiệp.

Công cụ điều tra sự cố

Các công cụ kiểm soát hoạt động trực tuyến như ghi âm các cuộc trao đổi, ghi lại nội dung màn hình theo thời gian thực, giám sát thao tác bàn phím, quay video qua webcam và tạo sơ đồ luồng thông tin cùng các biểu đồ kết nối giúp ghi lại các sự cố bảo mật theo từng bước. Công cụ Task Manager và các công cụ tìm kiếm sự cố tự động giúp nâng cao hiệu quả làm việc của đội ngũ an toàn thông tin.

Các yếu tố trí tuệ nhân tạo (AI)

Hệ thống tự động nhận diện khuôn mặt người dùng và xác định liệu máy tính có đang được sử dụng bởi chủ sở hữu hay không. Risk Monitor cũng phát hiện các nỗ lực chụp ảnh màn hình máy tính bằng điện thoại thông minh và để lại dấu vết số thông qua các watermark đặc biệt để xác định nguồn gốc của sự cố rò rỉ dữ liệu tiềm ẩn.

Mô hình triển khai trên đám mây

Tất cả các thành phần của Risk Monitor có thể được triển khai trên nền tảng đám mây (đám mây của SearchInform hoặc bất kỳ dịch vụ đám mây bên thứ ba nào) mà không ảnh hưởng đến chức năng của hệ thống. Đây là phương thức triển khai tiết kiệm chi phí và thời gian.

Tích hợp với các sản phẩm SearchInform khác

Giải pháp SearchInform được tích hợp liền mạch với SIEM và FileAuditor, giúp nâng cao mức độ an toàn thông tin và nhận thức về rủi ro trong doanh nghiệp, rút ngắn thời gian phản ứng đối với sự cố và cho phép điều tra toàn diện các hành vi vi phạm.

SearchInform TimeInformer

Đối với một số nhân viên, việc có mặt tại nơi làm việc không đồng nghĩa với việc thực hiện đúng các nhiệm vụ được giao. Luôn có những trường hợp thiếu trách nhiệm như nghỉ hút thuốc hoặc uống cà phê quá thường xuyên, trò chuyện với đồng nghiệp, dành thời gian trên mạng xã hội, đi làm muộn hoặc về sớm.

HOẠT ĐỘNG CỦA NHÓM

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

TimeInformer quét các máy tính trong doanh nghiệp và giúp bạn xác định:

Những người vi phạm kỷ luật lao động như đi làm muộn, về sớm, nghỉ hút thuốc hoặc uống cà phê quá thường xuyên

Những nhân viên lãng phí thời gian khi trò chuyện, mua sắm trực tuyến, chơi game hoặc tham gia các hoạt động gây xao nhãng khác

Những nhân viên làm việc riêng hoặc nhận việc ngoài trong thời gian làm việc được công ty trả lương

Những nhân viên không hài lòng, có thể kích động đồng nghiệp chống lại doanh nghiệp, hoặc những người bị kiệt sức do khối lượng công việc nặng nề hoặc do công việc nhàm chán

TimeInformer theo dõi thời gian làm việc và thời gian nhàn rỗi của nhân viên, đồng thời thu thập dữ liệu về các phần mềm họ sử dụng trong ngày. Hệ thống ghi lại tất cả các trang web mà họ truy cập và phân loại chúng theo các nhóm như trang hẹn hò, mua sắm trực tuyến, tin tức, chương trình truyền hình và các nhóm khác. Thông tin này sau đó được sử dụng để đánh giá năng suất làm việc thực tế của nhân viên dựa trên các tiêu chí được xác định trước.

GIÁM SÁT THEO THỜI GIAN THỰC

TimeInformer có thể hoạt động không chỉ ở chế độ nền mà còn ở nhiều chế độ giám sát chủ động. Chương trình kết nối với màn hình máy tính và micro, cho phép quan sát hoạt động trên các máy trạm của nhân viên theo thời gian thực.

Hệ thống có thể ghi lại các cuộc trao đổi quan trọng với đối tác và khách hàng, ghi nhận cả âm thanh và hoạt động trên màn hình theo thời gian thực. Giải pháp cũng cho phép giám sát trực tiếp đồng thời tối đa 16 màn hình của nhân viên.

TimeInformer giám sát các máy tính trong doanh nghiệp và giúp bạn xác định nhu cầu mua sắm hoặc bảo trì thêm thiết bị phần cứng.

HỖ TRỢ RA QUYẾT ĐỊNH QUẢN LÝ

33 báo cáo được cấu hình sẵn trong TimeInformer giúp triển khai nhanh chóng, cho phép phát hiện nhanh các nhân viên làm việc kém hiệu quả, hỗ trợ tối ưu hóa quy trình làm việc, tổ chức đội ngũ và đảm bảo các mục tiêu được thực hiện.

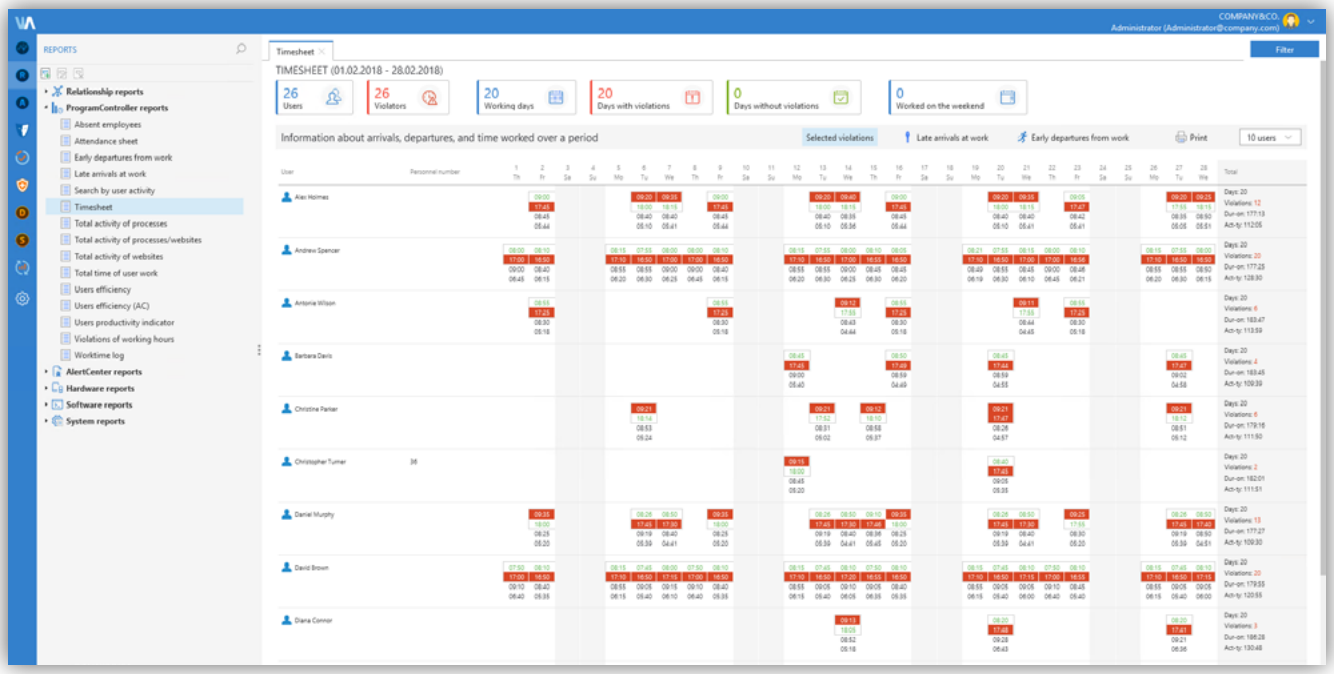
TimeInformer cung cấp các nhóm báo cáo sau:

- Báo cáo về hoạt động của người dùng trong các ứng dụng và trên các trang web
- Báo cáo về chương trình, bao gồm lịch sử cài đặt và gỡ cài đặt phần mềm
- Báo cáo về thiết bị, bao gồm thông tin về phần cứng được cài đặt trên máy tính và các thay đổi trong cấu hình của chúng

Các báo cáo và thông báo có thể được tùy chỉnh dễ dàng. Hệ thống tự động thông báo cho quản trị viên khi phát hiện vi phạm chính sách.

GIAO DIỆN THÂN THIỆN VỚI NGƯỜI DÙNG

Giao diện web cho phép các nhà quản lý giám sát nhân viên từ bất kỳ đâu trên thế giới. Quyền truy cập vào báo cáo và các chức năng quản trị được cấu hình theo vai trò và trách nhiệm. Hệ thống gửi cảnh báo tự động qua email để thông báo cho quản trị viên về bất kỳ hoạt động đáng ngờ nào của nhân viên.



Bảng chấm công trên giao diện web

ƯU ĐIỂM

- Được bảo vệ khỏi việc xóa và được cấu hình để cảnh báo khi có bất kỳ nỗ lực xóa dữ liệu nào
- Giám sát hoạt động của người dùng ngay cả khi họ làm việc từ xa hoặc đang đi công tác
- Giao diện web cho phép truy cập kết quả giám sát từ bên ngoài văn phòng
- Tích hợp với các sản phẩm của SearchInform, hỗ trợ thực hiện các cuộc điều tra nội bộ

SearchInform Managed Security Services

Dịch vụ MSS của SearchInform đảm bảo bảo vệ liên tục dữ liệu nhạy cảm và giúp nâng cao hiệu quả hoạt động của doanh nghiệp.

KHI SỬ DỤNG DỊCH VỤ, KHÁCH HÀNG SẼ NHẬN ĐƯỢC:

- Ngăn chặn rò rỉ dữ liệu
- Giám sát năng suất làm việc của nhân viên và phát hiện các dấu hiệu lười biếng có hệ thống
- Phát hiện gian lận trong doanh nghiệp (hoa hồng bất hợp pháp, làm việc ngoài giờ cho bên khác)
- Bảo vệ bí quyết công nghệ và tài sản trí tuệ
- Giảm thiểu rủi ro mất nhân sự chủ chốt
- Điều tra các sự cố an ninh thông tin

CÁCH THỨC HOẠT ĐỘNG

1. **Chuyên gia an ninh thông tin cấu hình hệ thống theo yêu cầu của khách hàng.**
2. **Chuyên gia an ninh thông tin thực hiện giám sát, ngăn chặn sự cố và thông báo cho khách hàng trong các tình huống khẩn cấp.**
3. **Khách hàng nhận được các báo cáo chi tiết.**
4. **Doanh nghiệp trở nên an toàn hơn, minh bạch hơn và hoạt động hiệu quả hơn.**

DÙNG THỬ MIỄN PHÍ 30 NGÀY VỚI ĐẦY ĐỦ TÍNH NĂNG

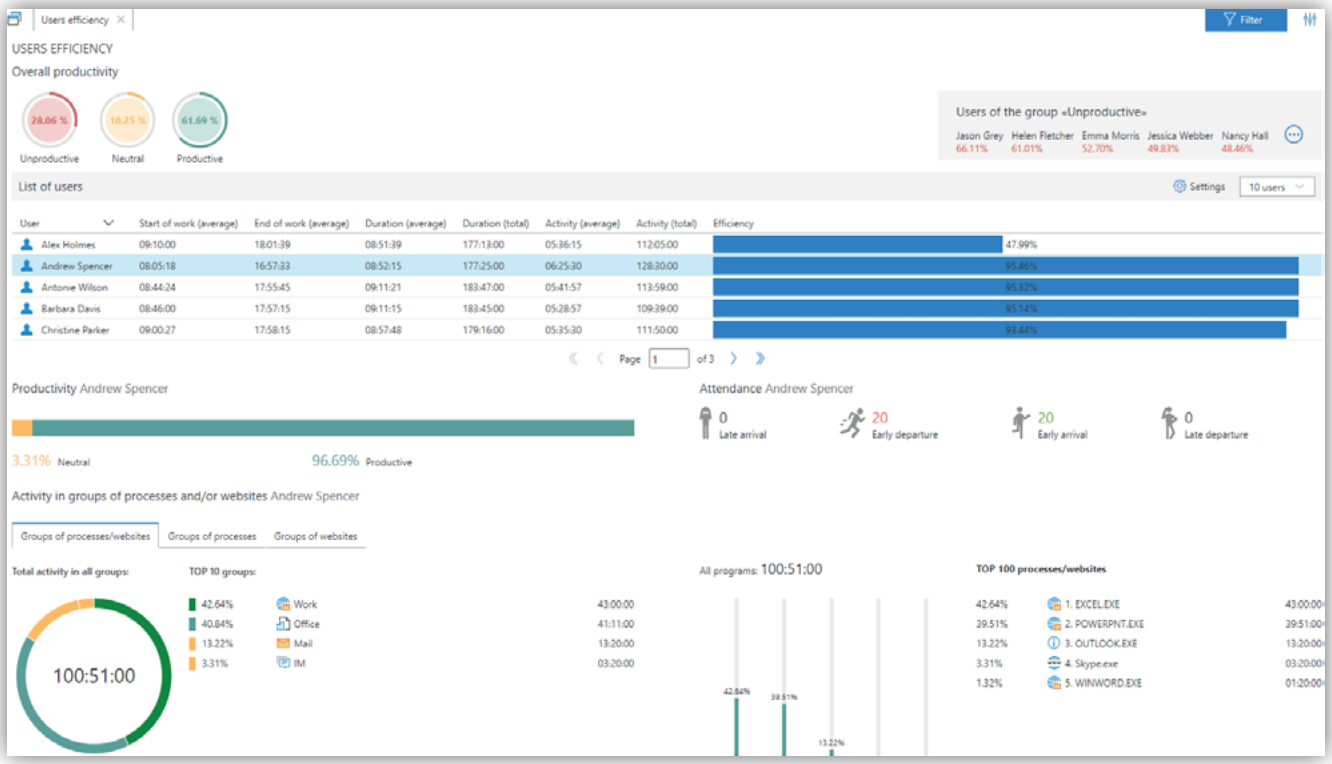
Trong thời gian dùng thử miễn phí, bạn sẽ thực hiện đánh giá hệ thống của tổ chức, xác định các vấn đề về bảo vệ dữ liệu, nhận được kết quả thực tế, nhận tư vấn từ chuyên gia về việc nâng cao bảo mật doanh nghiệp, và đánh giá liệu MSS có đáp ứng các yêu cầu của bạn hay không.

NHIỆM VỤ – GIẢI PHÁP

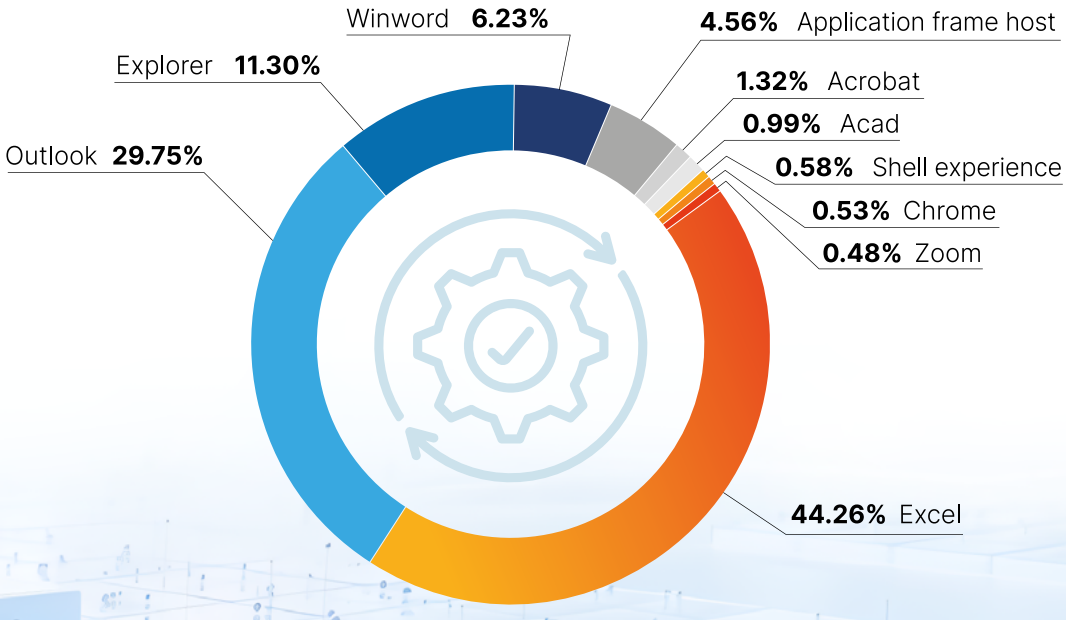
Khách hàng có được cái nhìn đầy đủ về các hoạt động thực tế trong tổ chức thông qua các báo cáo toàn diện dựa trên dữ liệu.

Date	Employees involved	Comments	Link to documents
External Devices			
05/06/2024	John Smith	An employee connected personal USB flash drive to the corporate computer and attempted to copy large amount of data. The process was blocked, and data leakage was prevented. The investigation revealed that the employee had tried to copy customer database and sell it later to a competitor.	full factual Info
Data Leakages			
21/06/2024	Ömer Aydın	Analysis of correspondance in corporate WhatsApp revealed a data leak incident. The employee discussed an oncoming deal with representative of the market competitor, they communicated via IM. Lately the employee has shared a few commercial documents related to the deal with the competitor via WhatsApp.	full factual Info
01/07/2024	Barabara Davis	Employee intended to breach data: he created an email draft in personal Google mailbox using corporate laptop and attached confidential financial data and files (incl. phone bill). This would enable the insider to access the data outside of the corporate perimeter after some time without even sending the email.	full factual Info
Document Forgery			
05/07/2024	Danielle Murphy	Procurement department employee forges incoming commercial offers from suppliers with the help of graphic editor. He changes the sums mentioned in the offers.	full factual Info
Side companies			
14/07/2024	Bhupesh Ghoshal	The signs of document forgery were detected. The investigation revealed that the employee used to edit documents of third-party company, which turned out to be the competitor, and the employee was its co-founder.	full factual Info
20/07/2024	Khalid Mustafa	Charter documents of some third-party company were found on the computer of one employee from the finance department. The investigation revealed that the founder of this company is this employee's wife. Evidence that this company is the regular supplier can be found in the link to documents section.	full factual Info
Job Search			
29/07/2024	Jamil Faridi	There was found evidence that one employee is currently actively checking vacancies to apply for a job. The employee was receiving job-related emails at: [redacted]	full factual Info
Misuse of Corporate Resources			
13/08/2024	Hasan Demir	An employee uses corporate laptop to play games. The online games use various types of unwanted cookies and show ads which may damage the company equipment.	full factual Info
Risk Group Employees			
20/08/2024	Elif Kaya	One employee from the sales department spends a few hours a week on gambling websites.	full factual Info
23/08/2024	Jane Doe	Correspondence of one employee revealed she had heavy debts and a few people demanded debt repayment from her. The employee works in the finance department, so the risks must be eliminated.	full factual Info
Sabotage			
02/09/2024	Christopher Turner	A resigning employee attempted to harm the company by deleting some confidential data without the possibility of recovery. The employee's attempt was successfully prevented. View detailed report to find out which data exactly the employee tried to delete.	full factual Info

KHẢ NĂNG HIỂN THỊ TOÀN DIỆN MỌI QUY TRÌNH KINH DOANH

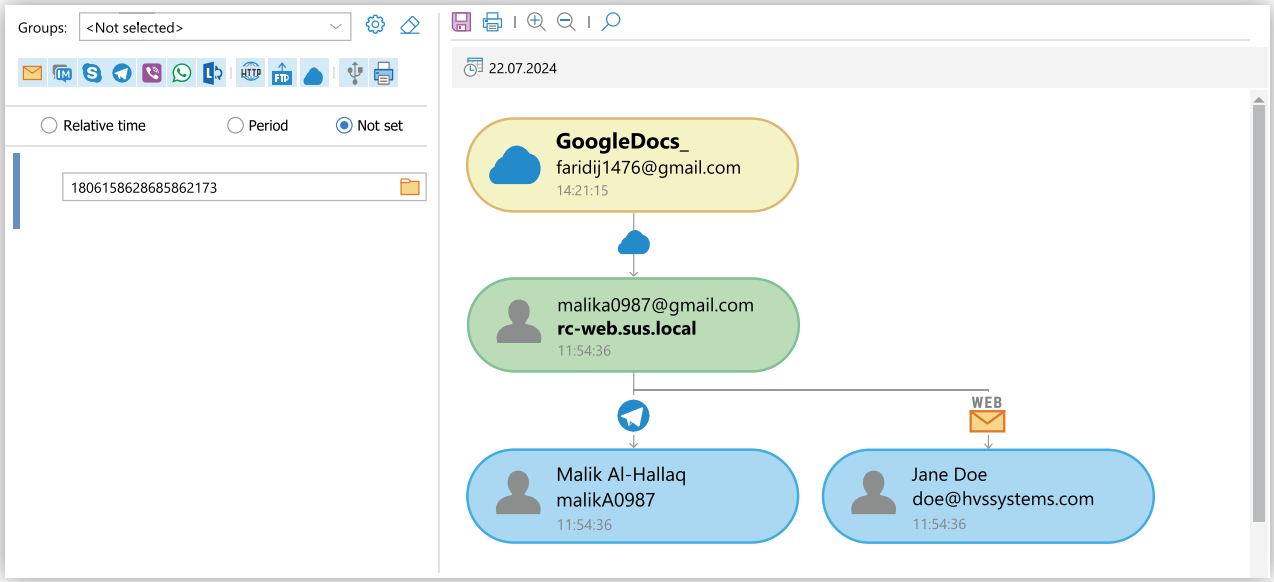


Báo cáo về hiệu suất làm việc của người dùng



Các quy trình được sử dụng nhiều nhất

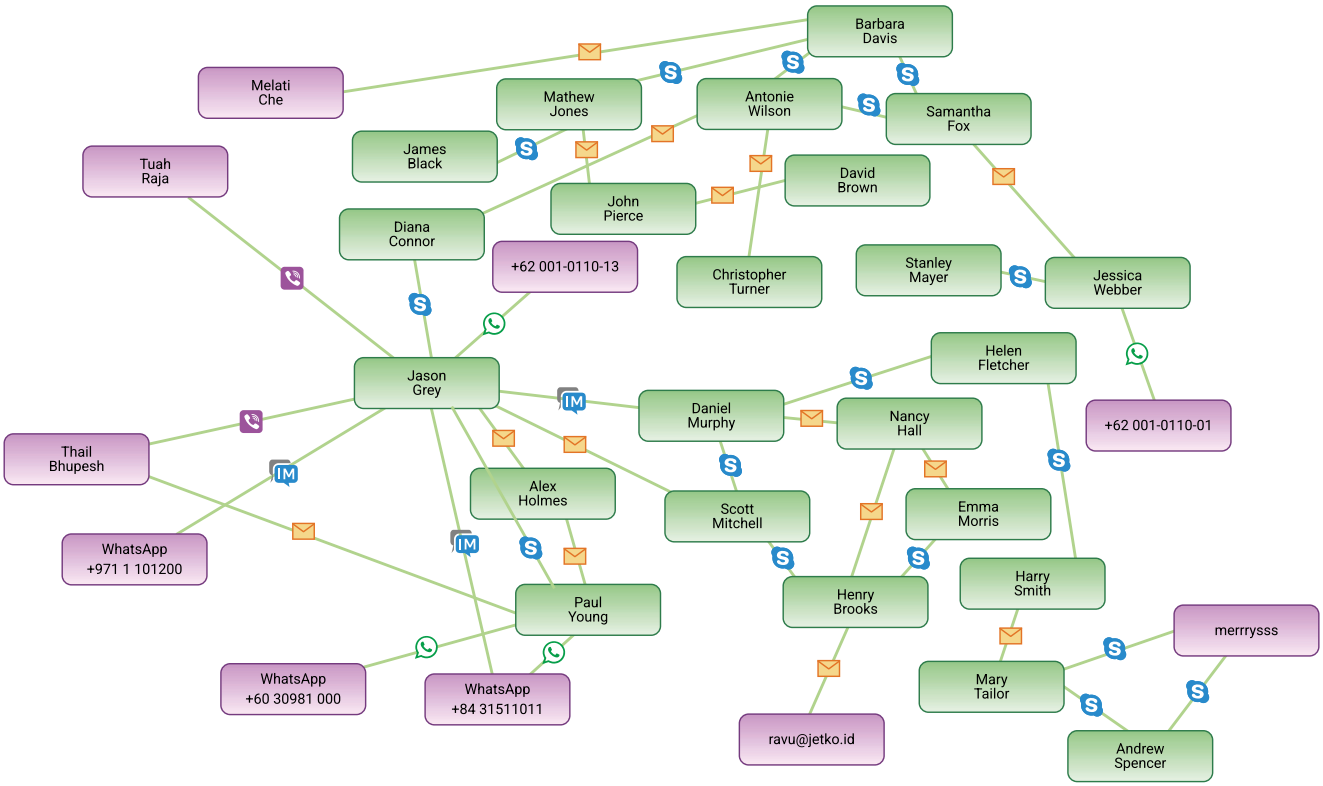
PHÂN TÍCH CHÍNH XÁC



Lộ trình nội dung

Một báo cáo tài chính đã bị rò rỉ. Báo cáo lộ trình nội dung cho thấy đường đi của tài liệu bị rò rỉ.

Báo cáo các mối liên kết xác định tất cả người dùng liên quan đến sự cố an ninh.



Báo cáo kết nối người dùng

ƯU ĐIỂM

- **Tiết kiệm ngân sách** Không cần phải:
  - mua sắm thiết bị
  - trả phí bản quyền phần mềm và hỗ trợ
  - tuyển dụng hoặc duy trì chuyên gia an ninh thông tin

- **Kết quả mà không phát sinh chi phí nhân sự**

  Cung cấp khả năng bảo vệ nâng cao mà không cần đội ngũ chuyên gia nội bộ, khắc phục khó khăn trong việc tìm kiếm nhân sự đủ trình độ trên thị trường.

- **Tính chuyên nghiệp khách quan**

  Đội ngũ chuyên gia phân tích của chúng tôi không có mối quan hệ cá nhân với nhân viên của bạn, giúp loại bỏ yếu tố thiên vị trong quá trình điều tra.

- **Hiệu quả tức thì**

  Phát hiện nhanh các lỗ hổng (kết quả ban đầu thường xuất hiện trong thời gian dùng thử miễn phí 1 tháng).

- **Chuyên môn sâu rộng**

  Các chuyên gia phân tích sử dụng cơ sở tri thức được xây dựng từ hơn 4.000 trường hợp khách hàng, cấu hình giải pháp bảo vệ phù hợp với từng ngành nghề.

Tích hợp Microsoft 365

Các giải pháp SearchInform được tích hợp hoàn toàn và liền mạch với Microsoft 365

Xu hướng chuyển sang sử dụng các dịch vụ đám mây đang gia tăng. Khi các ứng dụng và dữ liệu được chuyển lên đám mây, với thông tin và chức năng có thể truy cập thông qua các phiên bản chạy trên trình duyệt, các phương pháp bảo vệ endpoint truyền thống không còn đủ hiệu quả.

Microsoft 365 là một trong những dịch vụ đám mây phổ biến nhất. SearchInform đã phát triển giải pháp bảo vệ chuyên biệt cho Microsoft 365 nhằm bảo vệ dữ liệu doanh nghiệp cho khách hàng.

- Việc tích hợp được thực hiện thông qua Graph API, cung cấp cho khách hàng quyền truy cập đầy đủ vào tất cả các chức năng quan trọng của giải pháp bảo mật.
- Các giải pháp SearchInform cung cấp khả năng bảo vệ trên toàn bộ các dịch vụ Microsoft 365, bao gồm Word, Excel, PowerPoint, Outlook, Teams, SharePoint, OneDrive, v.v.

CÁCH THỨC HOẠT ĐỘNG

Thông qua tích hợp liền mạch, các tệp và thông tin được chuyển tới các dịch vụ Microsoft 365 (bao gồm Outlook) sẽ được SearchInform FileAuditor và SearchInform DLP phân tích và bảo vệ trực tiếp trên máy chủ.

Các cơ chế bảo vệ chính cho Microsoft 365 bao gồm:

- Mô hình bảo vệ không cần cài đặt agent giúp bảo vệ hiệu quả trong môi trường ranh giới doanh nghiệp ngày càng mờ nhạt;
- Sử dụng phân tích dựa trên nội dung để xác định chính xác nội dung của tài liệu;
- Phân tích các nhãn phân loại được gán thông qua Microsoft Information Protection;
- Môi trường bảo vệ thống nhất cho đám mây, Windows, macOS và Linux;
- Hỗ trợ quét các tệp trong SharePoint.

TÍCH HỢP FILEAUDITOR VỚI MICROSOFT 365

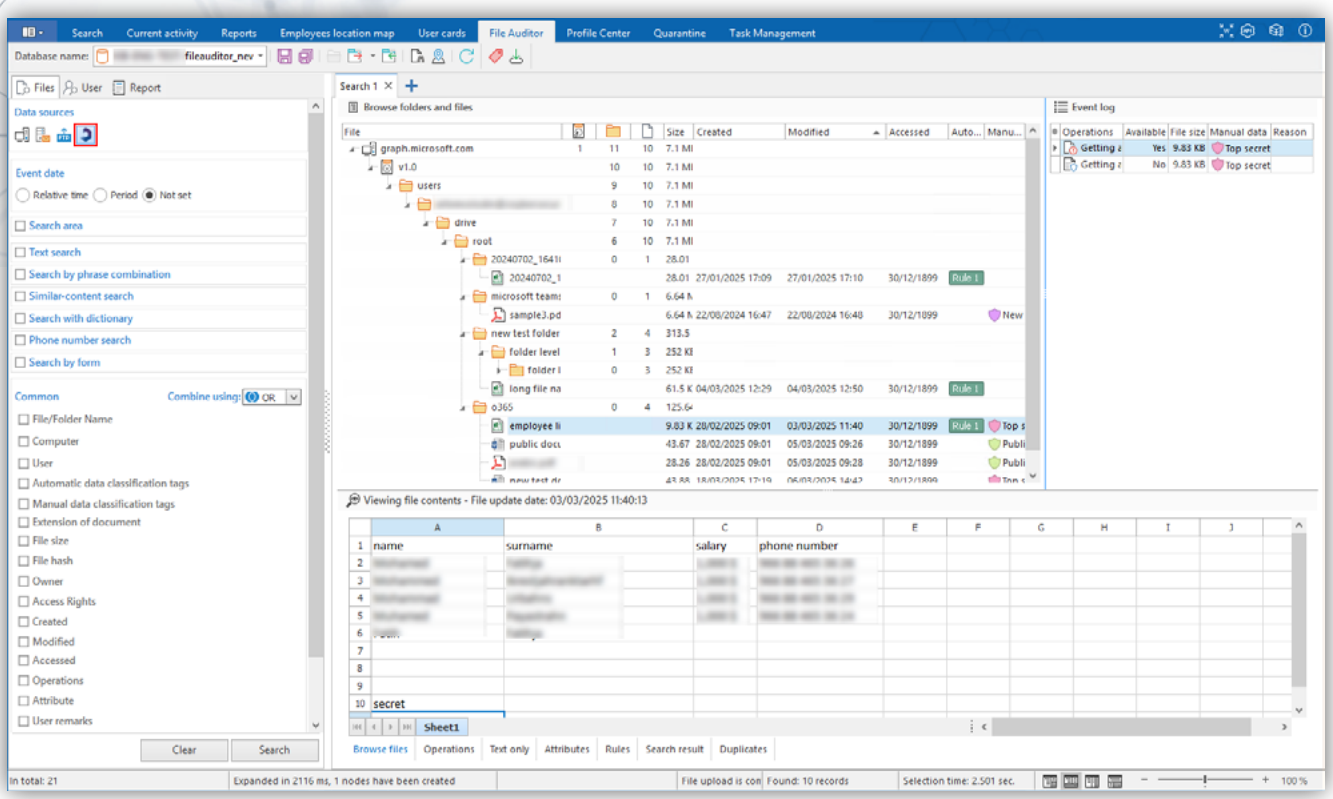
Khi làm việc với Microsoft 365, FileAuditor giám sát mọi hoạt động của người dùng trong phạm vi hệ thống doanh nghiệp.

Hệ thống truy cập tất cả các không gian làm việc trong Microsoft 365 mà người dùng tương tác.

Giải pháp quét các không gian làm việc này và phân loại các tệp được lưu trữ bằng phân tích dựa trên nội dung.

Đồng thời, FileAuditor tự động sắp xếp các tệp vào các danh mục. Ví dụ, khi một tệp xuất hiện trong cuộc trò chuyện Teams, giải pháp sẽ tạo một thư mục riêng có tên “Microsoft Teams Chat Files” để lưu trữ.

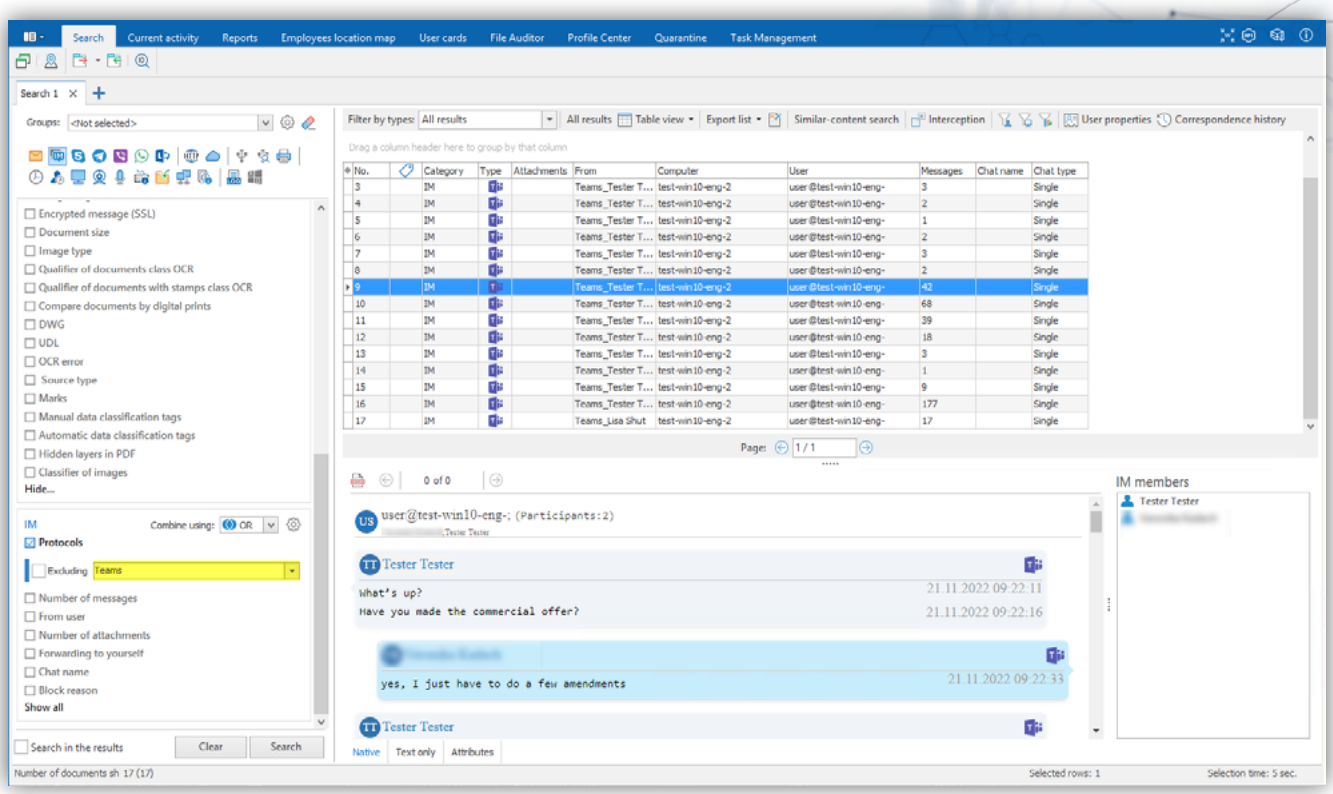
FileAuditor phân tích tất cả các tệp và gán nhãn độ nhạy dựa trên nội dung tài liệu, loại thông tin và mức độ nhạy cảm. Điều này cho phép đánh giá chính xác mức độ quan trọng của dữ liệu và thực thi các chính sách bảo mật phù hợp.



Kết quả quét Microsoft 365 bằng FileAuditor

TÍCH HỢP DLP VỚI MICROSOFT 365

Việc tích hợp SearchInform DLP với Microsoft 365 cung cấp cho người dùng quyền truy cập đầy đủ vào tất cả các chức năng DLP tiêu chuẩn.



1 Giải pháp kiểm soát việc truyền dữ liệu trên tất cả các dịch vụ Microsoft 365.

2 Nguyên tắc hoạt động dựa trên việc phân tích ngữ cảnh và nội dung của tệp để xác định loại dữ liệu, mức độ bảo mật và liệu dữ liệu đó có chịu sự áp dụng của các chính sách bảo mật cụ thể hay không (việc tích hợp với FileAuditor giúp tăng độ chính xác và giảm chi phí vận hành DLP).

3 Tất cả các khả năng phân tích nâng cao truyền thống và điều tra số vẫn được duy trì. Chuyên gia an ninh thông tin nhận được thông tin chi tiết đầy đủ về sự kiện, bao gồm tin nhắn gốc, các tệp được truyền (ở định dạng ban đầu), cũng như thông tin người gửi và người nhận.

SearchInform SIEM

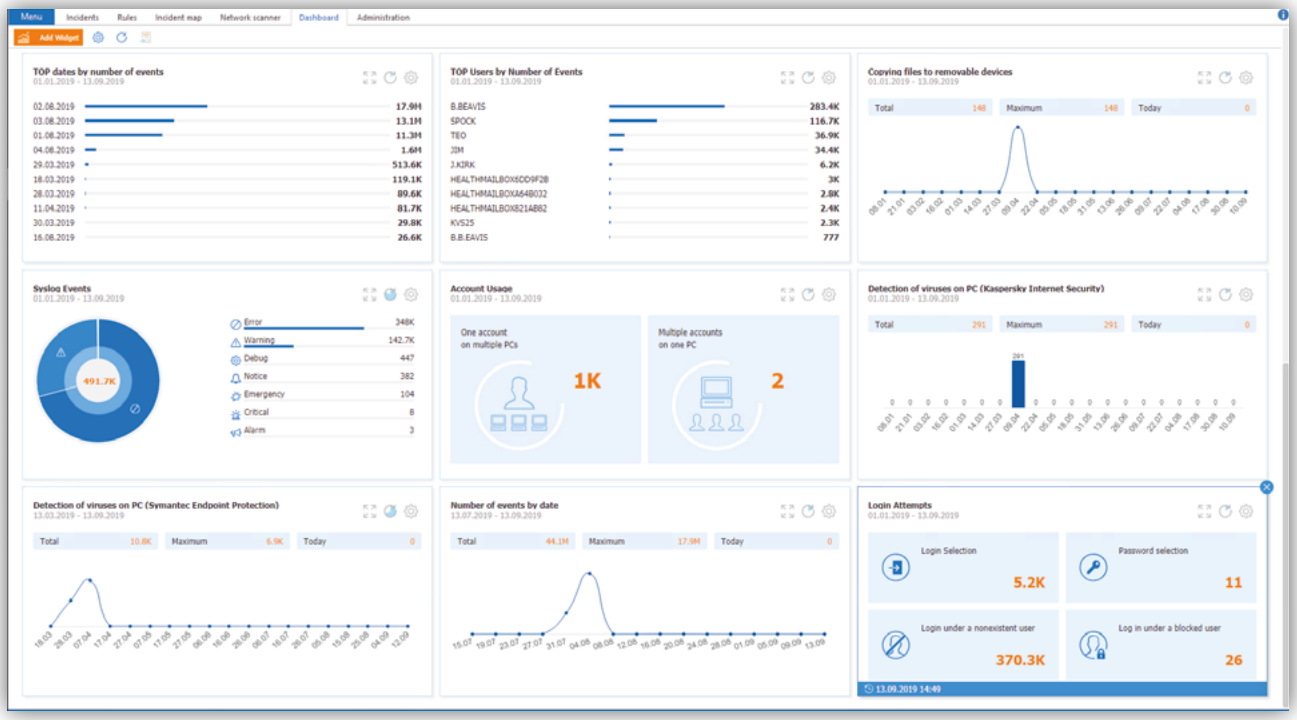
- SIEM SẴN SÀNG SỬ DỤNG
- CÁC QUY TẮC TƯƠNG QUAN ĐƯỢC TẠO CHỈ TRONG 2 LẦN NHẤP CHUỘT

Cơ sở hạ tầng CNTT của doanh nghiệp hiện đại bao gồm nhiều hệ thống quan trọng: tường lửa, hệ điều hành, máy chủ email, cơ sở dữ liệu và các thiết bị mạng.

Các hệ thống này là mục tiêu chính của các tác nhân tấn công, do đó cần các biện pháp bảo mật chuyên biệt.

Giám sát tự động các sự kiện an ninh

SearchInform SIEM là một giải pháp toàn diện cho việc thu thập, phân tích sự kiện an ninh theo thời gian thực và phản ứng với các sự cố. Hệ thống tổng hợp dữ liệu từ nhiều nguồn, thực hiện phân tích nâng cao, tự động ghi nhận các sự cố và cảnh báo cho nhân sự được chỉ định.



Bảng điều khiển thống kê sự kiện

SearchInform SIEM phát hiện:

- Các đợt bùng phát virus và các trường hợp nhiễm riêng lẻ
- Các nỗ lực truy cập trái phép
- Tấn công dò mật khẩu bằng brute-force
- Các tài khoản vẫn hoạt động của nhân viên đã nghỉ việc
- Lỗi cấu hình phần cứng
- Vi phạm nhiệt độ vận hành cho phép
- Xóa dữ liệu quan trọng
- Sử dụng tài nguyên doanh nghiệp ngoài giờ trái phép
- Xóa máy ảo và snapshot
- Kết nối phần cứng trái phép vào hạ tầng CNTT
- Thay đổi chính sách Group Policy
- Truy cập từ xa trái phép qua TeamViewer hoặc các công cụ khác
- Các sự kiện bảo mật quan trọng của hệ thống
- Sự cố và lỗi của hệ thống thông tin

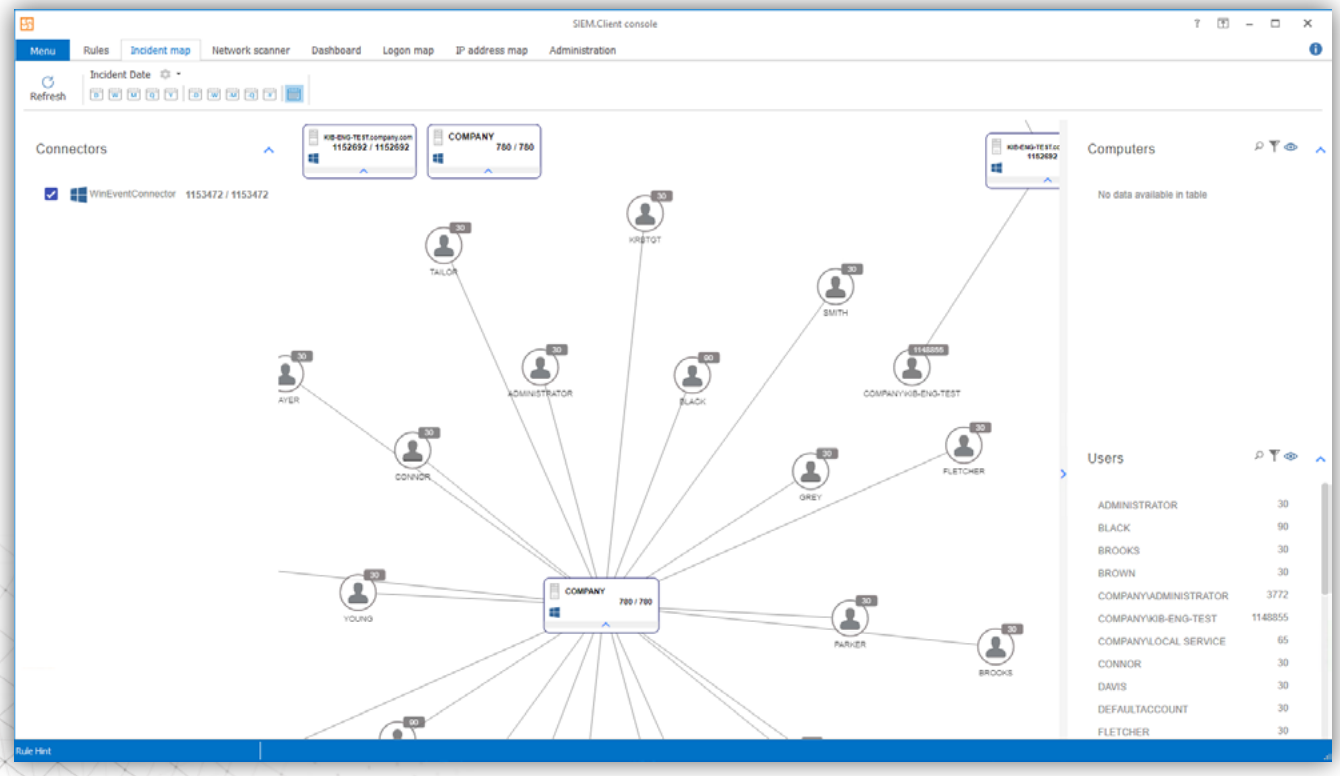
CÁC QUY TẮC TƯƠNG QUAN ĐƯỢC ĐỊNH NGHĨA SẴN

Sau khi cài đặt, hệ thống cung cấp cho đội ngũ an ninh thông tin hơn 350 quy tắc bảo mật sẵn sàng sử dụng, khả năng tùy chỉnh đầy đủ và các công cụ tạo quy tắc linh hoạt (bao gồm tùy chỉnh user connector). Các nhóm an ninh có thể chỉnh sửa các quy tắc có sẵn và tạo quy tắc tùy chỉnh, kết hợp chúng một cách hiệu quả để nâng cao mức độ bảo mật.

Các quy tắc được định nghĩa sẵn sử dụng các thành phần hạ tầng quan trọng sau:

- Hệ điều hành
- Máy chủ email
- Bộ điều khiển miền và máy trạm
- Máy chủ và máy trạm Linux
- Hệ quản trị cơ sở dữ liệu (DBMS)
- Hệ thống DLP
- Máy chủ tệp
- Môi trường ảo hóa
- Phần mềm diệt virus
- Tường lửa và thiết bị bảo mật mạng
- Tất cả các thiết bị tương thích với syslog

Các quy tắc tương quan chéo có thể được cấu hình để phát hiện các sự cố an ninh phức tạp bằng cách phân tích các sự kiện liên kết từ nhiều nguồn dữ liệu khác nhau.



Màn hình hiển thị sự cố

Các quy tắc tương quan được định nghĩa sẵn trong SearchInform SIEM:

Giám sát máy chủ thư điện tử

- Các nỗ lực truy cập hộp thư trái phép
- Thay đổi quyền sở hữu hộp thư
- Cấp quyền truy cập hộp thư trái phép

Bảo vệ môi trường ảo hóa

- Các mẫu đăng nhập/đăng xuất VMware/ VWview đáng ngờ
- Các lần nhập mật khẩu sai lặp lại
- Xóa snapshot trái phép

Bảo mật bộ điều khiển miền và máy trạm

- Kích hoạt/tạo tài khoản tạm thời
- Một tài khoản hoạt động trên nhiều thiết bị cùng lúc
- Tấn công dò mật khẩu brute-force và sử dụng mật khẩu đã hết hạn

Kiểm soát truy cập tài nguyên

- Truy cập trái phép vào các tệp quan trọng
- Gán quyền truy cập tạm thời cho tệp/thư mục
- Các mẫu truy cập tệp bất thường từ nhiều người dùng

CÁCH HỆ THỐNG HOẠT ĐỘNG

1. Thu thập sự kiện từ nhiều nguồn phần mềm và phần cứng khác nhau: thiết bị mạng, phần mềm bên thứ ba, công cụ bảo mật và hệ điều hành.
2. Phân tích các sự kiện và tạo sự cố theo các quy tắc, phát hiện mối đe dọa bằng cách xác định mối quan hệ (tương quan, bao gồm tương quan chéo) giữa các sự kiện và/hoặc sự cố.
3. Tự động thông báo cho nhân viên an ninh khi sự cố xảy ra.
4. Chuẩn hóa và chi tiết hóa các sự cố để phục vụ điều tra thêm: xác định loại sự cố và nguồn gốc, và khi tích hợp với Active Directory sẽ xác định người dùng.

ƯU ĐIỂM

- Triển khai nhanh và cấu hình sẵn (có thể vận hành trong một ngày với kết quả ngay lập tức).
- Giao diện trực quan và thân thiện với người dùng, không yêu cầu kỹ năng lập trình để tạo các quy tắc tương quan.
- Yêu cầu phần cứng thấp, cấp phép minh bạch và chi phí sở hữu tối ưu.
- Phân tích được cấu hình sẵn bao gồm hơn 350 quy tắc sẵn dùng dựa trên kinh nghiệm từ nhiều ngành khác nhau.
- Điều tra sự cố: phân tích các vụ việc dựa trên một hoặc nhiều sự cố.

Việc tích hợp với Risk Monitor giúp tăng cường an ninh thông tin bằng cách hỗ trợ điều tra sự cố toàn diện từ đầu đến cuối với đầy đủ bằng chứng.

LIÊN HỆ

CHÂU MỸ LATINH

Email: s.bertoni@searchinform.com

BẮC PHI

Email: m.sayari@searchinform.com

ĐÔNG NAM Á

Email: order@searchinform.com

NGA

Email: info@searchinform.ru

KAZAKHSTAN

Email: e.matushenok@searchinform.ru

TRUNG ĐÔNG VÀ BẮC PHI

Email: uae@searchinform.com

THỔ NHĨ KỲ

Email: salesturkiye@searchinform.com

VIỆT NAM

Email: vn@searchinform.com

Hãy thử ngay và truy cập các tài nguyên hữu ích tại **vn.searchinform.com**

KHÁCH HÀNG CỦA CHÚNG TÔI