SEARCHINFORM

Tuân thủ các quy định về bảo vệ dữ liệu tại Việt Nam

Tìm hiểu cách các giải pháp của SearchInform giúp đảm bảo tuân thủ các quy định về bảo vệ dữ liệu tại Việt Nam

MỤC LỤC

Luật số: 91/2025/QH15

YÊU CẦU:

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân.

4. Triển khai hiệu quả và đồng bộ các biện pháp, giải pháp về thể chế, kỹ thuật và nhân sự phù hợp nhằm bảo vệ dữ liệu cá nhân.

5. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, đồng thời xử lý kịp thời và nghiêm minh mọi hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân.

Cách SearchInform giúp đáp ứng các yêu cầu:

SearchInform cung cấp một bộ công cụ bảo vệ dữ liệu toàn diện, tạo thành một hệ sinh thái thống nhất.

FileAuditor, một giải pháp thuộc lớp DCAP, mang lại các khả năng phát hiện dữ liệu, phân loại dữ liệu và quản lý chi tiết quyền truy cập của người dùng.

Risk Monitor, một nền tảng DLP thế hệ mới, giúp ngăn chặn mất mát dữ liệu, thay đổi và chỉnh sửa trái phép. Đồng thời, giải pháp còn cung cấp các tính năng như đóng dấu (watermark), điều tra số (e-forensics) và các khả năng phân tích nâng cao.

SearchInform SIEM thu thập nhật ký và bản ghi từ nhiều giải pháp bảo mật khác nhau, áp dụng các quy tắc tương quan và phát hiện các mối đe dọa cũng như sự cố tiềm ẩn trong toàn bộ môi trường CNTT doanh nghiệp.

SEARCHINFORM
INFORMATION SECURITY

YÊU CẦU:

Điều 7. Hành vi bị nghiêm cấm

1. Xử lý dữ liệu cá nhân nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Cản trở hoạt động bảo vệ dữ liệu cá nhân.

3. Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để thực hiện hành vi vi phạm pháp luật.

4. Xử lý dữ liệu cá nhân trái quy định của pháp luật.

5. Sử dụng dữ liệu cá nhân của người khác, cho người khác sử dụng dữ liệu cá nhân của mình để thực hiện hành vi trái quy định của pháp luật.

6. Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

7. Chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân.

Cách SearchInform giúp đáp ứng các yêu cầu:

Các giải pháp của SearchInform cung cấp khả năng bảo vệ toàn diện trước việc sử dụng sai mục đích dữ liệu. FileAuditor, một giải pháp thuộc lớp DCAP, giúp phát hiện các tệp nhạy cảm, phân loại chúng theo một sơ đồ đã xác định và tự động quản lý quyền truy cập, từ đó hạn chế việc lộ dữ liệu do cấu hình sai.

Risk Monitor, một nền tảng DLP thế hệ mới, giám sát tất cả các kênh truyền dữ liệu chính, ngăn chặn các sự cố do vô ý hoặc cố ý liên quan đến mất mát, chỉnh sửa, thay đổi, chia sẻ hoặc phá hủy dữ liệu.

Các giải pháp của SearchInform có thể được cấu hình để tạo "bản sao bóng" (shadow copy) của các tệp quan trọng, cho phép khôi phục dữ liệu về trạng thái ban đầu.

YÊU CẦU:

Điều 18. Các hoạt động khác trong xử lý dữ liệu cá nhân

1. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên thứ ba lưu trữ dữ liệu cá nhân theo hình thức phù hợp với hoạt động của mình và có biện pháp bảo vệ dữ liệu cá nhân trong quá trình lưu trữ theo quy định của pháp luật.

Cách SearchInform giúp đáp ứng các yêu cầu:

FileAuditor, một giải pháp thuộc lớp DCAP, được thiết kế để bảo vệ dữ liệu lưu trữ (data at rest). Giải pháp tiến hành quét toàn bộ hạ tầng CNTT, bao gồm cả các dịch vụ đám mây, phân tích các tệp và phân loại chúng theo một sơ đồ phân loại đã được xác định. Sơ đồ phân loại này có thể được cấu hình để đáp ứng các yêu cầu của từng ngành cụ thể.

Giải pháp hỗ trợ cả phân loại tự động và gắn nhãn thủ công. FileAuditor cũng quản lý quyền truy cập của người dùng, hạn chế quyền truy cập vào các dữ liệu và tài liệu mật.

YÊU CẦU:

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên thứ ba phát hiện vi phạm quy định về bảo vệ dữ liệu cá nhân có thể gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của chủ thể dữ liệu cá nhân thì phải thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất là 72 giờ kể từ khi phát hiện hành vi vi phạm. Trường hợp bên xử lý dữ liệu cá nhân phát hiện hành vi vi phạm phải thông báo kịp thời cho bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân.

Cách SearchInform giúp đáp ứng các yêu cầu:

Risk Monitor, một nền tảng DLP thế hệ mới, ghi lại hoạt động của người dùng liên quan đến tệp và cung cấp một loạt các khả năng phân tích, bao gồm công nghệ tìm kiếm nâng cao và định tuyến nội dung.

Giải pháp bao gồm các mẫu báo cáo giúp đội ngũ an ninh nhanh chóng thông báo cho các bên liên quan về sự cố, với các thông tin chi tiết như loại dữ liệu bị lộ, số lượng bản ghi bị ảnh hưởng và thời điểm xảy ra.

Ngoài ra, Risk Monitor còn tích hợp một mô-đun quản lý sự cố chuyên biệt, cho phép phân công nhiệm vụ trong đội ngũ an ninh và tối ưu hóa quy trình báo cáo.

YÊU CẦU:

Điều 25. Bảo vệ dữ liệu cá nhân trong tuyển dụng, quản lý, sử dụng người lao động

1. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân trong tuyển dụng lao động được quy định như sau:

c) Phải xóa, hủy thông tin đã cung cấp của người dự tuyển trong trường hợp không tuyển dụng, trừ trường hợp có thỏa thuận khác với người đã dự tuyển;

2. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân trong quản lý, sử dụng người lao động được quy định như sau:

a) Tuân thủ quy định của Luật này, pháp luật về lao động, việc làm, pháp luật về dữ liệu và quy định khác của pháp luật có liên quan;

b) Dữ liệu cá nhân của người lao động phải lưu trữ trong thời hạn theo quy định của pháp luật hoặc theo thỏa thuận;

c) Phải xóa, hủy dữ liệu cá nhân của người lao động khi chấm dứt hợp đồng, trừ trường hợp theo thỏa thuận hoặc pháp luật có quy định khác.

Cách SearchInform giúp đáp ứng các yêu cầu:

FileAuditor, một giải pháp thuộc lớp DCAP, hỗ trợ quản lý lưu giữ dữ liệu. Giải pháp giúp phát hiện các tệp chứa dữ liệu cá nhân, chẳng hạn như CV hoặc bản quét giấy tờ tùy thân, đồng thời xác định tất cả các bản sao của các tệp này, cho phép xóa chúng theo đúng các yêu cầu pháp lý.

YÊU CẦU:

Điều 26. Bảo vệ dữ liệu cá nhân đối với thông tin sức khỏe và trong hoạt động kinh doanh bảo hiểm

1. Việc bảo vệ dữ liệu cá nhân đối với các thông tin sức khỏe và trong hoạt động kinh doanh bảo hiểm được quy định như sau:

b) Áp dụng đầy đủ quy định về bảo vệ dữ liệu cá nhân, quy định khác của pháp luật có liên quan.

3. Tổ chức, cá nhân phát triển ứng dụng về y tế, ứng dụng về kinh doanh bảo hiểm phải tuân thủ đầy đủ quy định về bảo vệ dữ liệu cá nhân.

Cách SearchInform giúp đáp ứng các yêu cầu:

Các giải pháp của SearchInform, như FileAuditor và Risk Monitor, giúp bảo vệ thông tin y tế khỏi việc bị tiết lộ, phá hủy hoặc chỉnh sửa do vô ý hoặc cố ý.

Các công cụ này giám sát tất cả các kênh truyền dữ liệu chính, bao gồm email, thiết bị USB di động và các dịch vụ đám mây.

YÊU CẦU:

Điều 27. Bảo vệ dữ liệu cá nhân trong hoạt động tài chính, ngân hàng, hoạt động thông tin tín dụng

1. Tổ chức, cá nhân hoạt động trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng có trách nhiệm sau đây:

a) Thực hiện đầy đủ quy định về bảo vệ dữ liệu cá nhân nhạy cảm, các tiêu chuẩn an toàn, bảo mật trong hoạt động tài chính, ngân hàng theo quy định của pháp luật;

d) Thông báo cho chủ thể dữ liệu cá nhân trong trường hợp lộ, mất thông tin về tài khoản ngân hàng, tài chính, tín dụng, thông tin tín dụng.

2. Tổ chức, cá nhân thực hiện hoạt động thông tin tín dụng có trách nhiệm tuân thủ quy định của Luật này; áp dụng các biện pháp phòng, chống truy cập, sử dụng, tiết lộ, chỉnh sửa trái phép dữ liệu cá nhân của khách hàng; có giải pháp khôi phục dữ liệu cá nhân của khách hàng trong trường hợp bị mất; bảo mật trong quá trình thu thập, cung cấp, xử lý dữ liệu cá nhân của khách hàng phục vụ đánh giá thông tin tín dụng.

Cách SearchInform giúp đáp ứng các yêu cầu:

SearchInform FileAuditor kết hợp nhiều biện pháp bảo vệ quan trọng trong một giải pháp duy nhất. Giải pháp quản lý quyền truy cập dữ liệu, hạn chế việc lộ các tệp mật và phát hiện các tệp được cấu hình sai. Đồng thời, hệ thống tạo các bản sao "shadow copy" của những tệp chứa dữ liệu nhạy cảm, cho phép khôi phục trong trường hợp bị phá hủy hoặc chỉnh sửa trái phép.

Risk Monitor cung cấp cho đội ngũ an ninh một bộ công cụ điều tra toàn diện. Giải pháp trang bị mô-đun quản lý sự cố, cho phép khởi tạo điều tra, phân công nhiệm vụ trong nhóm và chia sẻ thông tin. Bên cạnh đó, hệ thống duy trì một kho lưu trữ các thao tác với tệp, có thể được phân tích để tái dựng sự cố và xác định phạm vi rò rỉ dữ liệu.

YÊU CẦU:

Điều 31. Bảo vệ dữ liệu cá nhân đối với dữ liệu vị trí cá nhân, dữ liệu sinh trắc học

4. Việc bảo vệ dữ liệu sinh trắc học quy định như sau:

a) Cơ quan, tổ chức, cá nhân thu thập và xử lý dữ liệu sinh trắc học phải có biện pháp bảo mật vật lý đối với thiết bị lưu trữ và truyền tải dữ liệu sinh trắc học của mình; hạn chế quyền truy cập vào dữ liệu sinh trắc học; có hệ thống theo dõi để phòng ngừa, phát hiện hành vi xâm phạm dữ liệu sinh trắc học; tuân thủ quy định của pháp luật và tiêu chuẩn quốc tế có liên quan;

Cách SearchInform giúp đáp ứng các yêu cầu:

SearchInform FileAuditor cung cấp khả năng kiểm soát chi tiết quyền truy cập của người dùng đối với dữ liệu sinh trắc học. Để đảm bảo mức độ bảo vệ toàn diện, giải pháp có thể được kết hợp với các khả năng của Risk Monitor.

Nền tảng DLP thế hệ mới cho phép cấu hình các chính sách bảo mật cho từng người dùng, nhóm người dùng và máy trạm. Nhờ đó, tổ chức có thể thiết lập các quy tắc nhằm đảm bảo dữ liệu sinh trắc học chỉ được xử lý bởi một nhóm nhân viên hạn chế, trên các máy trạm chuyên dụng đặt tại các khu vực được bảo vệ về mặt vật lý.

YÊU CẦU:

Điều 37. Trách nhiệm của bên kiểm soát dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân

1. Trách nhiệm của bên kiểm soát dữ liệu cá nhân như sau:

c) Thực hiện biện pháp quản lý, kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân theo quy định của pháp luật, rà soát và cập nhật các biện pháp này khi cần thiết;

d) Thông báo hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định tại Điều 23 của Luật này;

2. Trách nhiệm của bên xử lý dữ liệu cá nhân như sau:

c) Thực hiện đầy đủ các biện pháp bảo vệ dữ liệu cá nhân theo quy định của Luật này và các quy định khác của pháp luật có liên quan;

Cách SearchInform giúp đáp ứng các yêu cầu:

Theo quy định của pháp luật, cả bên kiểm soát dữ liệu và bên xử lý dữ liệu đều phải triển khai các biện pháp bảo mật nhằm bảo vệ dữ liệu cá nhân. Các giải pháp của SearchInform bao gồm hơn 250 chính sách bảo mật được xây dựng sẵn, có thể được điều chỉnh theo yêu cầu của từng ngành hoặc phù hợp với các tiêu chuẩn quốc tế, qua đó giúp giảm thiểu nguồn lực cần thiết trong quá trình triển khai.

SearchInform cung cấp các khả năng bảo vệ dữ liệu toàn diện, từ ngăn chặn rò rỉ dữ liệu và phân loại dữ liệu đến điều tra sự cố và báo cáo nâng cao. Các giải pháp này bảo vệ dữ liệu một cách đáng tin cậy cho các tổ chức ở mọi quy mô, từ doanh nghiệp nhỏ đến các tập đoàn lớn.

SEARCHINFORM
INFORMATION SECURITY

CHẾ TÀI ĐỐI VỚI VIỆC KHÔNG TUÂN THỦ

YÊU CẦU:

Điều 8. Xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân

3. Mức phạt tiền tối đa trong xử phạt vi phạm hành chính đối với hành vi mua, bán dữ liệu cá nhân là 10 lần khoản thu có được từ hành vi vi phạm; trường hợp không có khoản thu từ hành vi vi phạm hoặc mức phạt tính theo khoản thu có được từ hành vi vi phạm thấp hơn mức phạt tiền tối đa quy định tại khoản 5 Điều này thì áp dụng mức phạt tiền theo quy định tại khoản 5 Điều này.

4. Mức phạt tiền tối đa trong xử phạt vi phạm hành chính đối với tổ chức có hành vi vi phạm quy định chuyển dữ liệu cá nhân xuyên biên giới là 5% doanh thu của năm trước liền kề của tổ chức đó; trường hợp không có doanh thu của năm trước liền kề hoặc mức phạt tính theo doanh thu thấp hơn mức phạt tiền tối đa theo quy định tại khoản 5 Điều này thì áp dụng mức phạt tiền theo quy định tại khoản 5 Điều này.

5. Mức phạt tiền tối đa trong xử phạt vi phạm hành chính đối với các hành vi vi phạm khác trong lĩnh vực bảo vệ dữ liệu cá nhân là 03 tỷ đồng.

6. Mức phạt tiền tối đa quy định tại các khoản 3, 4 và 5 Điều này được áp dụng đối với tổ chức; cá nhân thực hiện cùng hành vi vi phạm thì mức phạt tiền tối đa bằng một phần hai mức phạt tiền đối với tổ chức.

NGHỊ ĐỊNH 356/2025/NĐ-CP HƯỚNG DẪN LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

Theo Điều 4, dữ liệu cá nhân nhạy cảm bao gồm, nhưng không giới hạn ở:

a) Dữ liệu tiết lộ nguồn gốc chủng tộc hoặc dân tộc;

d) Tình trạng sức khỏe;

đ) Dữ liệu sinh trắc học và đặc điểm di truyền;

i) Thông tin về tên đăng nhập và mật khẩu để truy cập các tài khoản định danh điện tử cá nhân; hình ảnh của chứng minh nhân dân, căn cước công dân và thẻ định danh quốc gia;

k) Tên đăng nhập và mật khẩu của tài khoản ngân hàng; thông tin thẻ ngân hàng; lịch sử giao dịch của tài khoản ngân hàng; thông tin tài chính và tín dụng; và thông tin về hoạt động, lịch sử giao dịch liên quan đến tài chính, chứng khoán, bảo hiểm của khách hàng tại các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, công ty chứng khoán, công ty bảo hiểm và các tổ chức được cấp phép khác;

l) Dữ liệu về hành vi theo dõi và hoạt động sử dụng dịch vụ viễn thông, mạng xã hội, dịch vụ truyền thông trực tuyến và các dịch vụ khác trên không gian mạng;

YÊU CẦU:

Điều 8. Bảo vệ dữ liệu cá nhân trong hoạt động tài chính, ngân hàng, hoạt động thông tin tín dụng

1. Tổ chức, cá nhân hoạt động trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng có trách nhiệm áp dụng tiêu chuẩn, quy chuẩn kỹ thuật bảo vệ dữ liệu cá nhân; quy chuẩn kỹ thuật khử nhận dạng dữ liệu cá nhân, ẩn danh dữ liệu cá nhân được ban hành và áp dụng tại Việt Nam; thực hiện đánh giá tuân thủ các quy định về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần; ghi lại nhật ký toàn bộ hoạt động xử lý dữ liệu cá nhân.

Tổ chức, cá nhân hoạt động trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng là bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân khi xin sự đồng ý của chủ thể dữ liệu cá nhân phải đảm bảo nêu rõ:

a) Các mục đích xử lý dữ liệu cá nhân, bao gồm hoạt động chấm điểm, xếp hạng tín dụng, đánh giá thông tin tín dụng, đánh giá mức độ tín nhiệm về tín dụng nếu có;

b) Nguồn thu thập dữ liệu cá nhân và các bên thu thập, chia sẻ dữ liệu cá nhân liên quan;

c) Thời gian lưu trữ dữ liệu cá nhân;

d) Cơ chế, cách thức rút lại sự đồng ý và chính sách xóa, hủy dữ liệu cá nhân theo quy định.

3. Trong thời hạn không quá 72 giờ sau khi phát hiện lộ, mất dữ liệu nhạy cảm của chủ thể dữ liệu cá nhân trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng, tổ chức, cá nhân trực tiếp thu thập dữ liệu cá nhân của chủ thể dữ liệu có trách nhiệm thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân và chủ thể dữ liệu cá nhân. Nội dung thông báo cần đảm bảo tối thiểu các nội dung quy định tại khoản 1 Điều 28 Nghị định này.

Cách SearchInform giúp đáp ứng các yêu cầu:

Đối với Khoản 1, các giải pháp của SearchInform đáp ứng các yêu cầu về tiêu chuẩn và quy định áp dụng cho các tổ chức tài chính, ngân hàng và thông tin tín dụng. Để biết thêm thông tin chi tiết, vui lòng tham khảo phần tuân thủ dành cho các tổ chức tài chính.

Đối với Khoản 2, Risk Monitor – nền tảng DLP thế hệ mới – thu thập thông tin về các hoạt động xử lý dữ liệu và lưu trữ trong khoảng thời gian theo yêu cầu. Thông tin này có thể được sử dụng cho mục đích báo cáo tuân thủ và điều tra sự cố.

Đối với Khoản 3, các khả năng điều tra nâng cao của Risk Monitor và FileAuditor được hỗ trợ bởi các mẫu báo cáo, giúp tăng cường khả năng thu thập thông tin về sự cố của đội ngũ an ninh và tối ưu hóa quy trình báo cáo.

YÊU CẦU:

Điều 9. Bảo vệ dữ liệu cá nhân trong xử lý dữ liệu lớn

3. Cơ quan, tổ chức, cá nhân áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu lớn, bao gồm:

a) Áp dụng các biện pháp bảo đảm an ninh mạng, bảo mật dữ liệu, phòng chống thất thoát dữ liệu cá nhân trong quá trình lưu trữ, xử lý, truyền tải dữ liệu cá nhân;

b) Sử dụng phương thức xác thực mạnh, yêu cầu tối thiểu xác thực đa yếu tố (mật khẩu, mã PIN kết hợp với mật khẩu dùng một lần, thiết bị, ký số hoặc yếu tố sinh trắc học), phù hợp với mức độ nhạy cảm của dữ liệu cá nhân; phân quyền truy cập để đảm bảo chỉ những người có quyền mới có thể truy cập dữ liệu cá nhân;

c) Thực hiện mã hóa, ẩn danh dữ liệu cá nhân (quá trình tách các dữ liệu xác định một con người cụ thể để lưu trữ và bảo mật riêng biệt, các dữ liệu cá nhân sau quá trình này được sử dụng để xử lý mà không thể xác định một con người cụ thể) trong quá trình chuyển giao, cấp dữ liệu cá nhân, trừ trường hợp pháp luật chuyên ngành có quy định khác hoặc khi việc xử lý yêu cầu dữ liệu ở dạng bản rõ để phục vụ phòng, chống tội phạm, phòng chống rửa tiền, bảo đảm an ninh quốc gia, xử lý khiếu nại, tranh chấp của khách hàng. Trong các trường hợp này, cơ quan, tổ chức phải áp dụng bổ sung các giải pháp bảo mật để bảo đảm dữ liệu cá nhân không bị truy cập, sử dụng trái phép;

d) Thực hiện giám sát liên tục, sử dụng các công cụ giám sát để theo dõi hoạt động truy cập dữ liệu cá nhân và phát hiện các hành vi bất thường;

đ) Thực hiện kiểm tra, đánh giá định kỳ về an ninh mạng và bảo mật dữ liệu để phát hiện, ngăn chặn và khắc phục lỗ hổng bảo mật.

Cách SearchInform giúp đáp ứng các yêu cầu:

FileAuditor, một giải pháp thuộc lớp DCAP, bảo vệ dữ liệu lưu trữ (data at rest), trong khi Risk Monitor, một nền tảng DLP thế hệ mới, bảo vệ dữ liệu đang truyền (data in motion). Kết hợp lại, các giải pháp này tạo thành một môi trường bảo mật thống nhất, nâng cao tổng thể mức độ an toàn và khả năng chống chịu của hệ thống.

FileAuditor cung cấp các công cụ để cấu hình quyền truy cập dữ liệu của người dùng ở mức độ chi tiết. Giải pháp cho phép quản lý quyền truy cập đối với từng người dùng, nhóm người dùng và ứng dụng.

SearchInform DLP giám sát việc truyền dữ liệu trên tất cả các kênh giao tiếp kinh doanh chính. Giải pháp phát hiện các bất thường trên mạng, cho phép phản ứng nhanh chóng trước khi các sự cố leo thang.

YÊU CẦU:

Điều 12. Bảo vệ dữ liệu cá nhân trong điện toán đám mây

Các cơ quan, tổ chức, cá nhân có liên quan phải áp dụng các biện pháp kỹ thuật và tổ chức để ngăn chặn dữ liệu cá nhân bị truy cập trái phép khi triển khai dịch vụ điện toán đám mây.

Cách SearchInform giúp đáp ứng các yêu cầu:

Các giải pháp của SearchInform có thể được triển khai cả trong môi trường tại chỗ (on-premises) và môi trường đám mây. Ngoài ra, các giải pháp còn hỗ trợ triển khai trên các máy chủ chạy hệ điều hành Windows và Linux. Nhờ đó, SearchInform mang lại khả năng bảo vệ toàn diện với các tùy chọn triển khai linh hoạt.

YÊU CẦU:

Điều 28. Nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân, gồm:

a) Mô tả tính chất của việc vi phạm quy định về bảo vệ dữ liệu cá nhân, bao gồm: thời gian, địa điểm, hành vi, tổ chức, cá nhân, các loại dữ liệu cá nhân và số lượng dữ liệu liên quan;

Cách SearchInform giúp đáp ứng các yêu cầu:

SearchInform FileAuditor giám sát các hoạt động xử lý dữ liệu và thu thập nhật ký các thao tác với tệp.

Các nhật ký DLP bao gồm thông tin về thời điểm xảy ra sự cố, loại dữ liệu bị lộ và số lượng bản ghi bị ảnh hưởng.

LUẬT SỐ: 60/2024/QH15

YÊU CẦU:

Điều 13. Phân loại dữ liệu

1. Cơ quan nhà nước phải phân loại dữ liệu dựa trên yêu cầu quản trị, xử lý, bảo vệ dữ liệu, bao gồm:

a) Phân loại theo tính chất chia sẻ dữ liệu gồm: dữ liệu dùng chung, dữ liệu dùng riêng, dữ liệu mở;

b) Phân loại theo tính chất quan trọng của dữ liệu gồm: dữ liệu cốt lõi, dữ liệu quan trọng, dữ liệu khác;

c) Phân loại theo tiêu chí khác đáp ứng yêu cầu quản trị, xử lý, bảo vệ dữ liệu do chủ quản dữ liệu quyết định.

2. Chủ sở hữu dữ liệu, chủ quản dữ liệu không thuộc quy định tại khoản 1 Điều này phải phân loại dữ liệu theo quy định tại điểm b khoản 1 Điều này và được phân loại dữ liệu theo các tiêu chí khác.

3. Chính phủ quy định tiêu chí xác định dữ liệu cốt lõi, dữ liệu quan trọng.

Cách SearchInform giúp đáp ứng các yêu cầu:

Theo quy định tại Điều 13, dữ liệu được chủ sở hữu dữ liệu phân loại vào các danh mục đã xác định. Các công cụ DCAP như FileAuditor tự động phát hiện, gán nhãn và giám sát dữ liệu đã được phân loại dựa trên nội dung và ngữ cảnh; thực thi các chính sách thông qua việc theo dõi thao tác với tệp và quyền truy cập; đồng thời tích hợp với các hệ thống DLP để ngăn chặn việc di chuyển trái phép dữ liệu nhạy cảm.

Những khả năng kỹ thuật này giúp đảm bảo rằng việc phân loại dữ liệu không chỉ được thiết lập mà còn được thực thi và có thể kiểm toán trong hệ thống thông tin.

YÊU CẦU:

Điều 14. Hoạt động lưu trữ dữ liệu

1. Cơ quan nhà nước chịu trách nhiệm tổ chức lưu trữ dữ liệu bảo đảm an toàn.

2. Tổ chức, cá nhân không thuộc quy định tại khoản 1 Điều này là chủ sở hữu dữ liệu được quyền quyết định việc lưu trữ dữ liệu do mình thu thập, tạo lập, sở hữu; trường hợp lưu trữ dữ liệu cốt lõi, dữ liệu quan trọng phải bảo đảm tuân thủ theo quy định tại khoản 3 Điều 27 của Luật này.

Cách SearchInform giúp đáp ứng các yêu cầu:

Việc lưu trữ dữ liệu được triển khai trên hạ tầng bảo mật và sử dụng mã hóa. Các giải pháp DCAP và DLP được triển khai như những biện pháp kiểm soát kỹ thuật nhằm quản lý quyền truy cập vào dữ liệu lưu trữ, giám sát việc sử dụng và ngăn chặn việc trích xuất trái phép — đặc biệt đối với dữ liệu cốt lõi và dữ liệu quan trọng — qua đó hỗ trợ đáp ứng các yêu cầu bảo mật của Điều 14.

YÊU CẦU:

Điều 27. Bảo vệ dữ liệu

1. Biện pháp bảo vệ dữ liệu được áp dụng trong toàn bộ quá trình xử lý dữ liệu, bao gồm:

a) Xây dựng và tổ chức thực hiện chính sách, quy định bảo vệ dữ liệu;

b) Quản lý hoạt động xử lý dữ liệu;

c) Xây dựng và triển khai các giải pháp kỹ thuật;

d) Đào tạo, bồi dưỡng, phát triển, quản lý nguồn nhân lực;

đ) Các biện pháp bảo vệ dữ liệu khác theo quy định của pháp luật.

2. Cơ quan nhà nước phải bảo vệ dữ liệu trong ngành, lĩnh vực do mình quản lý, tuân thủ các chính sách chung về quốc phòng, an ninh; thiết lập hệ thống bảo vệ dữ liệu thống nhất để đánh giá rủi ro an ninh dữ liệu, giám sát và cảnh báo sớm.

3. Chủ sở hữu dữ liệu, chủ quản dữ liệu quản lý dữ liệu cốt lõi, dữ liệu quan trọng phải tuân thủ các quy định về bảo vệ dữ liệu.

4. Chính phủ quy định chi tiết Điều này.

Cách SearchInform giúp đáp ứng các yêu cầu:

Các giải pháp của SearchInform đảm bảo an toàn dữ liệu trong toàn bộ vòng đời xử lý dữ liệu, từ khi tạo lập đến khi xóa bỏ. Giải pháp bảo vệ dữ liệu nhạy cảm cả khi lưu trữ (data at rest) và khi truyền tải (data in motion).

Đối với Khoản 1(a), đội ngũ SearchInform cung cấp các công cụ linh hoạt để quản lý các giải pháp bảo mật. Việc xây dựng các quy tắc bảo mật không yêu cầu kỹ năng lập trình nâng cao. Các chuyên gia có thể sử dụng giao diện người dùng đồ họa (GUI) với các toán tử logic đơn giản để tạo chính sách phù hợp với các quy định liên quan.

Đối với Khoản 1(b), FileAuditor – một giải pháp DCAP – có thể được sử dụng để cấu hình quyền truy cập vào dữ liệu nhạy cảm cho nhân viên, đặc biệt là đối với dữ liệu cốt lõi và dữ liệu quan trọng. Giải pháp thiết lập các cơ chế kiểm soát bảo mật, đảm bảo rằng các dữ liệu mật không thể bị truy cập bởi những người không được phép.

Risk Monitor, một nền tảng DLP thế hệ mới, theo dõi dữ liệu đang truyền và ngăn chặn các nỗ lực đưa dữ liệu ra ngoài môi trường được bảo vệ. Giải pháp bảo vệ dữ liệu một cách đáng tin cậy trên máy trạm, dịch vụ đám mây và hệ thống lưu trữ mạng.

Khoản 1(c) quy định trực tiếp về sự cần thiết phải triển khai các giải pháp bảo mật. SearchInform cung cấp các công cụ bảo vệ có bản quyền với năng lực đã được kiểm chứng và hiệu quả. Giải pháp SearchInform DLP đã được đưa vào báo cáo Gartner Magic Quadrant.

Đối với Khoản 3, sự kết hợp giữa hệ thống DLP và DCAP mang lại khả năng bảo vệ dữ liệu toàn diện thông qua:

- kiểm soát truy cập mạnh mẽ
- giám sát liên tục
- ngăn chặn rò rỉ dữ liệu
- khả năng truy vết
- báo cáo

LUẬT AN NINH MẠNG SỐ 116/2025/QH15

YÊU CẦU:

Điều 5. Biện pháp bảo vệ an ninh mạng

1. Biện pháp bảo vệ an ninh mạng bao gồm:

...

h) Sử dụng giải pháp kỹ thuật để bảo vệ an ninh thông tin mạng, an ninh dữ liệu, hệ thống thông tin; ngăn chặn thông tin vi phạm pháp luật;

Cách SearchInform giúp đáp ứng các yêu cầu:

Nền tảng DLP thế hệ mới bảo vệ dữ liệu khỏi việc rò rỉ, thất thoát hoặc sử dụng trái phép bằng cách giám sát và ngăn chặn dữ liệu nhạy cảm rời khỏi hệ thống.

DCAP thực thi các chính sách truy cập dựa trên ngữ cảnh, giới hạn những ai có thể truy cập dữ liệu nhạy cảm và cách dữ liệu được sử dụng trong các ứng dụng và hệ thống.

YÊU CẦU:

Điều 12. Kiểm tra an toàn thông tin mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc danh mục hệ thống thông tin quan trọng liên quan đến an ninh quốc gia

2. Đối tượng kiểm tra an toàn thông tin mạng bao gồm:

a) Phần cứng, phần mềm và thiết bị số được sử dụng trong hệ thống thông tin;

b) Thông tin được lưu trữ, xử lý và truyền tải trong hệ thống thông tin;

c) Các biện pháp bảo vệ bí mật nhà nước, phòng ngừa và đấu tranh ngăn chặn việc lộ, mất bí mật nhà nước qua các kênh kỹ thuật.

Cách SearchInform giúp đáp ứng các yêu cầu:

Đối với Điểm a: Risk Monitor, một nền tảng dựa trên DLP thế hệ mới, cung cấp các báo cáo về tình hình sử dụng phần cứng và phần mềm trong toàn tổ chức. Điều này cho phép các đội ngũ an ninh giám sát việc sử dụng phần cứng, phát hiện những thay đổi trong cấu hình phần cứng và theo dõi các phần mềm mới được cài đặt.

Đối với Điểm b: FileAuditor, một giải pháp DCAP, thực hiện phát hiện dữ liệu bằng cách xác định và liệt kê các tài sản thông tin trong toàn tổ chức cũng như phân tích nội dung của chúng để phân loại các tệp có chứa dữ liệu nhạy cảm. Song song đó, công cụ DLP thế hệ mới giám sát dữ liệu đang trong quá trình truyền tải, đảm bảo rằng các bản ghi nhạy cảm không bị sửa đổi, phá hủy hoặc lộ ra ngoài một cách vô tình hay cố ý.

Đối với Điểm c: Các giải pháp của SearchInform có thể được sử dụng để hạn chế việc truyền tải dữ liệu bí mật bằng cách ngăn chặn các hoạt động truyền sang thiết bị USB hoặc ổ đĩa ngoài, tải lên qua web, chia sẻ qua mạng nội bộ hoặc in ấn. Risk Monitor cũng tăng cường bảo vệ dữ liệu bằng cách áp dụng hình mờ (watermark) lên các bản ghi nhạy cảm.

Ngoài ra, các giải pháp của SearchInform cung cấp công cụ cho giám định điện tử (e-forensics) và điều tra sự cố. Risk Monitor bao gồm một mô-đun quản lý sự cố chuyên dụng hỗ trợ quy trình điều tra trong nội bộ đội ngũ an ninh.

Các giải pháp của SearchInform cũng bao gồm các mẫu báo cáo được xây dựng sẵn, tạo điều kiện thuận lợi cho quá trình tuân thủ. Các báo cáo này đáp ứng cả yêu cầu pháp lý trong nước và quốc tế.

YÊU CẦU:

Điều 15. Phòng, chống gián điệp mạng; bảo vệ thông tin chứa bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng

1. Các hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

a) Chiếm đoạt, mua bán, thu giữ hoặc cố ý tiết lộ thông tin chứa bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư, gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức hoặc cá nhân;

b) Cố ý xóa, làm hư hỏng, làm mất hoặc thay đổi thông tin chứa bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa hoặc lưu trữ trên không gian mạng;

c) Cố ý thay đổi, hủy bỏ hoặc vô hiệu hóa các biện pháp kỹ thuật được xây dựng và áp dụng nhằm bảo vệ thông tin chứa bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

d) Đưa lên không gian mạng thông tin chứa bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái với quy định của pháp luật;

đ) Cố ý nghe lén, ghi âm hoặc ghi hình cuộc trò chuyện mà không được phép;

e) Các hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

2. Người quản lý hệ thống thông tin có trách nhiệm:

a) Kiểm tra an ninh mạng để phát hiện và loại bỏ mã độc, phần cứng độc hại; khắc phục các điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập trái phép hoặc các nguy cơ khác đe dọa an ninh mạng;

b) Triển khai các biện pháp quản lý và kỹ thuật nhằm phòng ngừa, phát hiện và ngăn chặn các hành vi gián điệp mạng hoặc xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin; đồng thời kịp thời gỡ bỏ thông tin liên quan đến các hành vi này.

Cách SearchInform giúp đáp ứng các yêu cầu:

Đối với Khoản 1(a), giải pháp DLP thế hệ mới của SearchInform ngăn chặn các hành vi lạm dụng quyền truy cập vào các tệp tin mật và chặn việc chia sẻ trái phép qua các kênh truyền thông doanh nghiệp. Danh sách các kênh được kiểm soát bao gồm nhưng không giới hạn ở:

- FTP
- HTTP(S)
- ứng dụng web
- dịch vụ đám mây (ví dụ: Microsoft 365)
- email
- ổ USB và thiết bị lưu trữ di động
- trình nhắn tin tức thời

Đối với Khoản 1(b), FileAuditor – một giải pháp DCAP – quản lý quyền truy cập của người dùng đối với dữ liệu nhạy cảm. Các chuyên gia an ninh có thể cấu hình quyền truy cập cho các nhóm người dùng, người dùng cá nhân và ứng dụng, xác định cách thức người dùng cụ thể được phép xử lý dữ liệu nhạy cảm. Ngoài ra, giải pháp còn tạo các bản sao lưu (shadow copies) của tệp tin, cung cấp thêm phương án sao lưu trong trường hợp dữ liệu bị sửa đổi trái phép.

Đối với Khoản 1(c), các giải pháp của SearchInform hoạt động ở chế độ ẩn, giúp tăng khả năng chống lại các hành vi can thiệp hoặc vô hiệu hóa hệ thống. Các giải pháp này không hiển thị với phần lớn người dùng, ngoại trừ đội ngũ an ninh thông tin. Đội ngũ SearchInform đặc biệt chú trọng đến tính chống chịu của các giải pháp bảo mật thông tin. Ví dụ, các nhãn bảo mật được nhúng trực tiếp vào tệp tin và người dùng không thể xóa bỏ. Các nhãn này vẫn được duy trì trên mọi bản sao của tệp, từ đó ngăn chặn các hành vi tìm cách vượt qua cơ chế kiểm soát bảo mật.

Đối với Khoản 1(d), giải pháp DLP ngăn chặn các hành vi truyền tải dữ liệu mật trái phép. Hệ thống giám sát tất cả các kênh truyền dữ liệu. Một ưu điểm nổi bật của các giải pháp SearchInform là công cụ DLP phân tích cả nội dung và ngữ cảnh của tệp tin. Điều này cho phép hệ thống chặn việc truyền dữ liệu trái phép không chỉ dựa trên các quy tắc được định nghĩa sẵn mà còn dựa trên bản chất của dữ liệu, bao gồm cả các hành vi cố tình né tránh phát hiện. Ví dụ, nếu một đối tượng xấu sửa đổi số thẻ ngân hàng hoặc số định danh quốc gia (chẳng hạn thay số "1" bằng chữ "one"), hệ thống vẫn có thể nhận diện được dữ liệu nhạy cảm.

Đối với Khoản 2(b), các giải pháp của SearchInform giám sát hoạt động mạng và phát hiện các hành vi đáng ngờ, chẳng hạn như cố gắng truyền tải dữ liệu hàng loạt hoặc đổi tên hàng loạt các tệp tin mật. Các giải pháp này cũng tích hợp công nghệ phân tích hành vi người dùng (User Behavior Analytics – UBA), giúp tăng cường khả năng phát hiện bằng cách nhận diện các hoạt động bất thường của người dùng.

YÊU CẦU:

Điều 26. Bảo đảm an toàn dữ liệu

1.Bảo đảm an toàn dữ liệu là tổng thể các biện pháp kỹ thuật, tổ chức và pháp lý nhằm bảo vệ dữ liệu và phòng ngừa, đấu tranh chống các hành vi xâm phạm an toàn dữ liệu.

2. Nội dung bảo đảm an toàn dữ liệu bao gồm:

a) Xây dựng chính sách và thiết lập quy trình về bảo đảm an toàn dữ liệu;

b) Áp dụng các biện pháp, tiêu chuẩn và quy chuẩn kỹ thuật theo quy định của pháp luật về an ninh mạng;

c) Sử dụng mật mã chuyên dụng và mật mã dân sự để bảo đảm an toàn dữ liệu;

d) Triển khai cơ chế kiểm soát chặt chẽ đối với nhân sự trực tiếp tham gia xử lý dữ liệu;

đ) Kiểm tra và đánh giá rủi ro định kỳ nhằm phát hiện, phòng ngừa và xử lý kịp thời các nguy cơ đe dọa an toàn dữ liệu;

e) Kiểm tra và đánh giá việc chuyển dữ liệu xuyên biên giới; các điều kiện bảo đảm an toàn dữ liệu trong các hệ thống thông tin quan trọng liên quan đến an ninh quốc gia, cơ sở dữ liệu, trung tâm dữ liệu và hệ thống lưu trữ dữ liệu;

g) Các nội dung khác theo quy định của pháp luật.

3. Chính phủ quy định chi tiết Khoản 2 Điều này và quy định trách nhiệm bảo đảm an toàn dữ liệu.for assurance of data security.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

Đối với Khoản 2(b), tất cả các giải pháp an ninh thông tin của SearchInform (DLP, DCAP và SIEM) đều cung cấp khả năng bảo vệ phù hợp với các tiêu chuẩn và quy định an ninh hiện hành. Các chuyên gia an ninh có thể sử dụng các quy tắc được xây dựng sẵn hoặc cấu hình các chính sách bảo mật tùy chỉnh phù hợp với yêu cầu pháp lý tại địa phương.

Đối với Khoản 2(d), hệ thống DCAP của SearchInform cho phép giới hạn quyền truy cập vào dữ liệu mật chỉ đối với những nhân sự được ủy quyền. Với FileAuditor, các chuyên gia an ninh có thể cấu hình cơ chế kiểm soát truy cập cho người dùng và ứng dụng, xác định cách thức dữ liệu được phép xử lý.

Đối với Khoản 2(đ), các giải pháp của SearchInform cung cấp nhật ký chi tiết về hoạt động của người dùng, cho phép giám sát liên tục các hoạt động hằng ngày và phát hiện các bất thường trong quá trình xử lý dữ liệu. Đội ngũ an ninh có thể phân tích các nhật ký này để chủ động xác định các mối đe dọa tiềm ẩn.

THÔNG TƯ QUI ĐỊNH VỀ AN TOÀN HỆ THỐNG THÔNG TIN TRONG HOẠT ĐỘNG NGÂN HÀNG

(CIRCULAR REGULATING INFORMATION SYSTEM SECURITY IN BANKING OPERATIONS)

YÊU CẦU:

Điều 4. Phân loại thông tin

Thông tin được xử lý và lưu trữ thông qua hệ thống thông tin được phân loại theo tính chất bảo mật như sau:

1. Thông tin công khai là thông tin được công bố cho mọi đối tượng mà không cần xác định danh tính hoặc địa chỉ cụ thể của các đối tượng đó;

2. Thông tin riêng tư (hoặc thông tin nội bộ) là thông tin được quản lý và truy cập theo cơ chế cấp quyền bởi một hoặc nhiều đối tượng có danh tính được xác định;

3. Thông tin cá nhân là thông tin xác định khách hàng và bao gồm các nội dung sau: thông tin tài khoản, thông tin tiền gửi, thông tin về tài sản ký gửi, thông tin giao dịch và các thông tin liên quan khác;

4. Thông tin mật bao gồm:

(i) Thông tin Mật, Tối mật và Tuyệt mật theo quy định của pháp luật về bảo vệ bí mật nhà nước;

(ii) Thông tin hạn chế truy cập theo quy định nội bộ của tổ chức.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

FileAuditor, giải pháp DCAP do SearchInform phát triển, thực hiện quét toàn bộ hạ tầng doanh nghiệp, bao gồm cả các dịch vụ đám mây, phân tích nội dung tệp tin và áp dụng các nhãn phân loại bảo mật dựa trên nội dung đó. Giải pháp cũng hỗ trợ việc gắn nhãn thủ công bởi người dùng hoặc các chuyên gia an ninh.

Hệ thống phân loại có thể được cấu hình để phù hợp với các quy định pháp luật tại địa phương cũng như các khung tiêu chuẩn an ninh quốc tế.

YÊU CẦU:

Điều 6. Quy định về an ninh thông tin

2. Quy định về an toàn thông tin tối thiểu phải bao gồm các nội dung cơ bản sau:

a) Quản lý tài sản công nghệ thông tin;

b) Quản lý nguồn nhân lực;

c) Bảo đảm an ninh vật lý và môi trường lắp đặt;

d) Quản lý vận hành và trao đổi thông tin;

đ) Quản lý truy cập;

e) Quản lý việc sử dụng dịch vụ công nghệ thông tin của bên thứ ba;

g) Quản lý việc tiếp nhận, phát triển và bảo trì hệ thống thông tin;

h) Quản lý sự cố an toàn thông tin;

i) Bảo đảm hoạt động liên tục của hệ thống thông tin;

k) Chế độ kiểm tra nội bộ và báo cáo.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

a) **Quản lý tài sản công nghệ thông tin**. Tài sản công nghệ thông tin bao gồm dữ liệu và cơ sở dữ liệu. Các tệp chứa nội dung nhạy cảm có thể được FileAuditor phân loại dựa trên nội dung của chúng. Risk Monitor – nền tảng DLP thế hệ mới – cũng cung cấp khả năng báo cáo về phần mềm và phần cứng, cho phép giám sát phần mềm đã cài đặt, phần cứng được sử dụng và việc sử dụng ứng dụng của từng người dùng.

b) **Quản lý nguồn nhân lực.** FileAuditor, một giải pháp DCAP, hỗ trợ quản lý chi tiết quyền truy cập của người dùng. Giải pháp này có thể được sử dụng để kiểm soát và phân phối quyền truy cập cho cả nhóm người dùng và người dùng cá nhân. Hệ thống cũng cho phép áp dụng các hạn chế cụ thể đối với nhân viên mới hoặc nhân sự sắp nghỉ việc.

d) **Quản lý vận hành và trao đổi thông tin.** Giải pháp DLP của SearchInform có thể được sử dụng để giám sát việc trao đổi thông tin và các luồng dữ liệu vận hành, cung cấp khả năng hiển thị đầy đủ đối với dữ liệu đang được truyền tải. FileAuditor quản lý quyền truy cập của người dùng, có thể được cấu hình cho từng người dùng hoặc ứng dụng, đồng thời phát hiện các trường hợp cấp quyền truy cập quá mức hoặc hoạt động bất thường.

Risk Monitor cũng cung cấp các khả năng phân tích và điều tra chuyên sâu. Các công cụ này cho phép đội ngũ an ninh phân tích chi tiết kho dữ liệu lưu trữ, tái dựng sự cố với độ chính xác cao và xác định phạm vi ảnh hưởng của sự cố. Giải pháp tích hợp sẵn mô-đun quản lý sự cố, hỗ trợ phân công nhiệm vụ trong đội ngũ an ninh, thu thập thông tin tập trung và tối ưu hóa quy trình báo cáo.

h) **Quản lý sự cố an toàn thông tin.** SearchInform SIEM có thể được sử dụng để thu thập nhật ký bảo mật từ nhiều hệ thống bảo vệ khác nhau và tương quan các sự kiện nhằm phát hiện sớm các sự cố. Hệ thống tích hợp với nhiều giải pháp bảo mật như tường lửa, phần mềm chống vi-rút và các nền tảng EDR/XDR. Nền tảng DLP thế hệ mới của SearchInform cũng cung cấp khả năng báo cáo nâng cao. Hệ thống cho phép đội ngũ an ninh nhanh chóng xác định chi tiết sự cố — chẳng hạn như thời điểm xảy ra, số lượng tệp bị ảnh hưởng và loại dữ liệu liên quan — đồng thời tạo báo cáo cho ban quản lý và các cơ quan có thẩm quyền liên quan.

TCVN ISO/IEC 27002

YÊU CẦU:

Điều khoản 8.2. Phân loại thông tin

8.2.1 Phân loại thông tin

Thông tin phải được phân loại dựa trên các yêu cầu pháp lý, giá trị, mức độ quan trọng và mức độ nhạy cảm đối với việc tiết lộ hoặc sửa đổi trái phép.

8.2.2 Gắn nhãn thông tin

Một bộ quy trình phù hợp về gắn nhãn thông tin phải được xây dựng và triển khai phù hợp với hệ thống phân loại thông tin được tổ chức áp dụng.

8.2.3 Xử lý tài sản

Các quy trình xử lý tài sản phải được xây dựng và triển khai phù hợp với hệ thống phân loại thông tin.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

Điều khoản 8.2.1

FileAuditor, một giải pháp thuộc nhóm DCAP, có thể được sử dụng để phân loại tài liệu trên toàn bộ hạ tầng của tổ chức. Giải pháp phân tích nội dung tệp tin và gán cấp độ phân loại dựa trên mức độ nhạy cảm của nội dung. Các chuyên gia an ninh có thể cấu hình các quy tắc phân loại phù hợp với yêu cầu của tổ chức. Tài liệu có thể được phân loại cả tự động và thủ công.

Điều khoản 8.2.2

FileAuditor cũng áp dụng các nhãn bảo mật cho tệp tin, có thể được gán tự động hoặc thủ công. Các nhãn này được nhúng ở cấp hệ thống tệp, bảo đảm người dùng không thể xóa chúng nhằm vượt qua các cơ chế kiểm soát bảo mật.

Điều khoản 8.2.3

Điều khoản này đề cập đến việc xử lý an toàn các tài sản thông tin trong toàn bộ vòng đời dữ liệu. Các giải pháp DCAP và DLP thế hệ mới của SearchInform bảo vệ dữ liệu cả khi lưu trữ và khi truyền tải.

FileAuditor quản lý quyền truy cập của người dùng đối với dữ liệu nhạy cảm, bảo đảm chỉ những nhân sự được ủy quyền mới có thể truy cập thông tin mật và việc truy cập này được giới hạn phù hợp với trách nhiệm công việc.

Giải pháp DLP thế hệ mới ngăn chặn cả các hành vi rò rỉ dữ liệu vô ý và cố ý bằng cách giám sát tất cả các kênh truyền dữ liệu chính, bao gồm FTP, email, Microsoft 365, thiết bị USB và hệ thống in ấn, đồng thời chặn các nỗ lực đưa dữ liệu ra ngoài trái phép.

Ngoài ra, giải pháp còn hỗ trợ cơ chế cấp quyền truy cập tạm thời và có kiểm soát đối với các kênh dữ liệu cụ thể. Nhân viên có thể gửi yêu cầu đến đội ngũ an ninh kèm theo lý do phù hợp để được cấp quyền tạm thời, giúp duy trì hoạt động kinh doanh liên tục trong khi vẫn đảm bảo các biện pháp kiểm soát an ninh.

YÊU CẦU:

9.2 Quản lý quyền truy cập của người dùng

9.2.5 Rà soát quyền truy cập của người dùng

Chủ sở hữu tài sản phải rà soát quyền truy cập của người dùng theo định kỳ.

9.2.6 Thu hồi hoặc điều chỉnh quyền truy cập

Quyền truy cập của tất cả nhân viên và người dùng bên ngoài phải được thu hồi khi chấm dứt hợp đồng lao động hoặc hợp đồng dịch vụ, hoặc được điều chỉnh khi có thay đổi liên quan.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

FileAuditor của SearchInform có thể được sử dụng như một công cụ hỗ trợ kiểm soát truy cập. Giải pháp này quản lý và phân phối quyền truy cập dữ liệu của người dùng, cho phép cấu hình các hạn chế truy cập cho từng người dùng hoặc nhóm người dùng.

Các quy tắc đặc biệt có thể được áp dụng đối với nhân viên mới và nhân sự nghỉ việc. Giải pháp cũng có thể được sử dụng để thu hồi hoàn toàn quyền truy cập dữ liệu đối với những nhân viên đã rời khỏi công ty.

YÊU CẦU:

9.4 Kiểm soát truy cập hệ thống và ứng dụng

9.4.1 Hạn chế truy cập thông tin

Việc truy cập thông tin và các chức năng của hệ thống ứng dụng phải được hạn chế phù hợp với chính sách kiểm soát truy cập hiện hành.

Người dùng chỉ được phép truy cập vào thông tin và các chức năng hệ thống mà họ được cấp quyền sử dụng, dựa trên nhu cầu công việc và trách nhiệm được giao.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

Các giải pháp của SearchInform có thể được sử dụng để đáp ứng các yêu cầu của Điều khoản 9.4.1.

FileAuditor có thể được sử dụng để hạn chế quyền truy cập của nhân sự đối với dữ liệu nhạy cảm. Giải pháp cũng có thể được cấu hình để giới hạn các ứng dụng được phép xử lý dữ liệu đó.

Hệ thống DLP bổ sung cho DCAP bằng cách kiểm soát cách dữ liệu nhạy cảm được xử lý trong các ứng dụng. Ví dụ, nhân viên có thể được phép mở và chỉnh sửa các bản thiết kế kỹ thuật, nhưng bị ngăn chặn tải chúng lên dịch vụ lưu trữ đám mây, xuất sang định dạng PDF hoặc đính kèm vào email.

YÊU CẦU:

12.4 Ghi nhật ký và giám sát

12.4.1 Ghi nhật ký sự kiện

Nhật ký sự kiện ghi lại hoạt động của người dùng, các ngoại lệ, lỗi và các sự kiện an toàn thông tin phải được tạo lập, lưu giữ và rà soát định kỳ.

Cách SearchInform hỗ trợ đáp ứng các yêu cầu:

Các giải pháp DLP và DCAP của SearchInform đều cung cấp khả năng hiển thị chi tiết đối với các tương tác của người dùng với dữ liệu. Đội ngũ an ninh có thể cấu hình các quy tắc để ghi lại ảnh chụp màn hình hoặc video màn hình khi nhân viên làm việc với dữ liệu nhạy cảm, từ đó giúp hiểu rõ hơn về các hoạt động xử lý dữ liệu.

SearchInform SIEM có thể được tích hợp liền mạch với FileAuditor và Risk Monitor. Giải pháp cũng bao gồm các bộ kết nối để tích hợp với các hệ thống bảo mật phổ biến khác, cho phép tương quan nhật ký và sự kiện một cách hiệu quả nhằm phát hiện sớm và ngăn chặn các sự cố an ninh.

SEARCHINFORM
INFORMATION SECURITY

SearchInform là một trong những nhà phát triển hàng đầu về các sản phẩm quản lý rủi ro và an toàn thông tin. Từ năm 2019, công ty đã cung cấp các dịch vụ bảo mật được quản lý (Managed Security Services). Trong hơn một thập kỷ, công ty đã đóng vai trò tiên phong về công nghệ, tập trung vào các mối đe dọa an ninh mạng hiện đại, bảo vệ doanh nghiệp và các cơ quan chính phủ trước nguy cơ đánh cắp dữ liệu, hành vi gây hại từ con người, vi phạm tuân thủ và kiểm toán không đầy đủ. Hơn 4.000 công ty thuộc các lĩnh vực kinh tế trọng yếu — từ ngân hàng và bán lẻ đến sản xuất máy móc và chế tạo máy bay chiến đấu — tin tưởng SearchInform trong việc triển khai giải pháp quản lý rủi ro toàn diện và hiệu quả, giúp bảo vệ trước các mối đe dọa ngày càng tinh vi và tránh các hậu quả nghiêm trọng.

SearchInform **DLP** giúp doanh nghiệp hiểu rõ dữ liệu của mình và triển khai các biện pháp kiểm soát chính xác tại những vị trí cần thiết nhằm bảo vệ công ty khỏi nguy cơ rò rỉ thông tin mật. SearchInform DLP giám sát tất cả các kênh truyền dữ liệu phổ biến, phân tích thông tin, phát hiện và ngăn chặn các hành vi vi phạm, đồng thời cung cấp báo cáo cho người phụ trách.

SearchInform **FileAuditor** là một giải pháp DCAP (kiểm toán và bảo vệ dữ liệu tập trung vào dữ liệu) được thiết kế nhằm hỗ trợ doanh nghiệp xác định thông tin nhạy cảm trong hệ thống tệp, kiểm toán các kho lưu trữ thông tin, phát hiện các vi phạm truy cập và theo dõi các thay đổi được thực hiện đối với dữ liệu quan trọng. Hệ thống bảo vệ các tài liệu mật trước những hành vi bất cẩn hoặc cố ý gây hại của nhân viên, đồng thời giúp tổ chức và quản lý hiệu quả các kho lưu trữ tệp tin.

SearchInform **SIEM** là hệ thống thu thập và phân tích các sự kiện an ninh theo thời gian thực, giúp xác định các sự cố an toàn thông tin và hỗ trợ phản ứng kịp thời đối với các sự cố đó. Hệ thống thu thập thông tin từ nhiều nguồn khác nhau, thực hiện phân tích, ghi nhận sự cố và gửi cảnh báo đến nhân sự phụ trách.

Nền tảng SearchInform **Risk Monitor** thực hiện phân tích theo thời gian thực, giúp nhận diện mọi sự kiện đang diễn ra trong hệ thống mạng. SearchInform Risk Monitor hỗ trợ doanh nghiệp xây dựng chương trình quản lý rủi ro và quy trình quản lý mối đe dọa nội bộ hiệu quả, giúp dự báo trước các rủi ro nội bộ tiềm ẩn trong tổ chức, đồng thời cung cấp các công cụ phục vụ điều tra số (forensics).

Bạn có thể tìm thêm nhiều tài liệu hữu ích liên quan đến các vấn đề an toàn thông tin trên website của SearchInform.

5th floor, East Tower Office, Lumiere Riverside Building, 277 Vo Nguyen Giap street, An Khanh Ward, Ho Chi Minh City

+84 869019330

vn@searchinform.com