Các Giải pháp Bảo vệ Dữ liệu của SearchInform:
Các Module Toàn diện và Mô tả Chi tiết

Để biết thêm chi tiết, vui lòng tham khảo phần mô tả.	TimeInformer	DLP	RiskMonitor	FileAuditor
Forensic	✗	✗	✓	✗
M365	✗	✗	✓	✓
MailController	✗	✓	✓	✗
IMController	✗	✓	✓	✗
DeviceController	✗	✓	✓	✗
CloudController	✗	✓	✓	✗
HttpController	✗	✓	✓	✗
FtpController	✗	✓	✓	✗
PrintController	✗	✓	✓	✗
MonitorController + Keylogger	✓	✗	✓	✗
Watermarks on screenshots	✓	✗	✓	✗
MicrophoneController	✓	✗	✓	✗
ProgramController	✓	✗	✓	✗
Data Classification	✗	✗	✗	✓
Files activities monitoring	✗	✗	✗	✓
Files access rights audit	✗	✗	✗	✓
Watermarks in files	✗	✗	✗	✓

Mô tả

Forensic DataBase lưu trữ tất cả các sự kiện "raw", dựa trên đó hệ thống phát hiện các incident. Ví dụ: phiên bản gốc của email, tin nhắn trong Telegram, tin nhắn thoại trong WhatsApp, tài liệu được tải lên cloud, v.v. Dữ liệu được lưu trữ không giới hạn thời gian và không phụ thuộc vào việc có phát hiện vi phạm security policies hay không. Forensic DataBase cho phép tìm kiếm thông tin dựa trên nội dung, đồng thời cung cấp khả năng áp dụng các security policies (chính sách bảo mật) đối với kho lưu trữ thông tin giao tiếp.

M365 là tích hợp với Microsoft 365 thông qua API độc quyền. Đối với DLP và Risk Monitor (RM), tính năng này cho phép bảo vệ các hoạt động trao đổi thông tin (tệp đính kèm, chat, nội dung văn bản) trong Teams Online và Exchange Online, bất kể người dùng truy cập nền tảng Microsoft 365 thông qua trình duyệt web hay ứng dụng desktop. Đối với FileAuditor (FA), việc tích hợp này cho phép phân loại mọi dữ liệu được người dùng tải lên hoặc xử lý trong hệ thống..

MailController — collection, categorization and quarantine of emails. Protects corporate and public email (gmail etc.). Protects email clients with classical protocols (IMAP, MAPI, SMTP's) and email in browser.

IMController — thu thập, phân loại và chặn các tin nhắn, cuộc gọi và tệp được truyền qua các phần mềm nhắn tin doanh nghiệp và phần mềm nhắn tin công cộng, bao gồm WhatsApp và Telegram.

DeviceController — thu thập, phân loại, chặn và áp dụng mã hóa bắt buộc đối với các tệp được truyền qua các cổng input/output trên các thiết bị lưu trữ dữ liệu.

CloudController — thu thập, phân loại và chặn các tệp được truyền đến các dịch vụ cloud hoặc phần mềm cộng tác (ví dụ: Zoom).

HttpController — thu thập, phân loại và chặn bất kỳ lưu lượng trình duyệt nào chưa được các controller khác ghi nhận.

FtpController — thu thập, phân loại và chặn lưu lượng FTP.

PrintController — thu thập, phân loại và chặn các tệp được gửi để in.

MonitorController + Keylogger — tạo screenshot và ghi lại màn hình người dùng, chụp ảnh hoặc quay video qua webcam, kiểm tra thao tác nhập từ bàn phím. Phát hiện việc chụp ảnh màn hình bằng thiết bị bên ngoài và đảm bảo nhận diện sinh trắc học của nhân viên thông qua khuôn mặt.

Watermarks on screenshots — hiển thị thông tin trên màn hình để bảo vệ chống lại việc chụp screenshot hoặc chụp ảnh màn hình.

MicrophoneController — thực hiện ghi âm từ microphone của PC với quá trình chuyển đổi và nhận dạng âm thanh thành văn bản theo thời gian thực.

ProgramController — đánh giá thời gian làm việc trong các chương trình và trình duyệt. Phân tích năng suất làm việc và hỗ trợ điều hướng hoạt động của người dùng trong các cuộc điều tra nội bộ.

Data Classification — phân loại tệp dựa trên nội dung đối với các tệp lưu trữ trên PC, trong LAN và trong hệ quản trị cơ sở dữ liệu. Hệ thống gắn các nhãn đặc biệt có thể được sử dụng cho mục đích kiểm tra (audit) cũng như làm tiêu chí để chặn quyền truy cập vào tệp.

File activity monitoring — ghi nhật ký hoạt động của các thao tác với tệp cục bộ và tệp trên mạng, hoạt động ở cấp driver và không yêu cầu kích hoạt các log tích hợp trong hệ điều hành.

File access rights audit — kiểm tra các quyền truy cập hiện tại và phát hiện các trường hợp thay đổi quyền truy cập đối với các đối tượng trong hệ thống tệp cục bộ và hệ thống tệp mạng.

Watermarks in files - a thêm văn bản hoặc ký hiệu vào tài liệu cụ thể để đánh dấu mức độ bảo mật của tài liệu.