SEARCHINFORM

منصة الحد
من التهديدات الداخلية

searchinform.com

1995 تاسست الشركة

أكثر من **3 000 000** جهاز حاسوب محميّ بواسطة برنامج SearchInform

أكثر من **4 000** عميل في جميع أنحاء العالم

6 منتجات تضمن حماية شاملة للبيانات ضد التهديدات السيبراني

2017

تم تضمين برنامج SearchInform في تقرير **Gartner Magic Quadrant**

2019

بدأت SearchInform في تقديم الخدمات المُدارة لحماية البيانات

2020

تم إطلاق حل SearchInform في السحابة

2010

تم افتتاح مركز التدريب

16 دورة تدريبية متقدمة لمتخصصي أمن المعلومات

2 دورتان أساسيتان في الأمن السيبراني للمستخدمين

2018-2020

أُقيمت سلسلة فعاليات **"The Road Show SearchInform"** في أمريكا اللاتينية، و الشرق الأوسط و شمال أفريقيا، و جنوب أفريقيا، و الهند، و إندونيسيا

2022-2023

أكثر من ٩ دول في شمال أفريقيا — SearchInform توسّع نطاق حضورها الإقليمي

2023

افتتحت SearchInform مكتبًا يركّز على تقديم الخدمات في دبي (الإمارات العربية المتحدة)

قامت **مجموعة Radicati** بتضمين دراسة "سوق منع فقدان بيانات المؤسسة، 2017-2021" في تقرير SearchInform.

المنتجات والخدمات

SearchInform FileAuditor

7-4

SearchInform DLP

9-8

SearchInform Risk Monitor

18-10

SearchInform TimeInformer

20-19

خدمات الأمن المُدارة من SearchInform

25-21

حلول SearchInform المتكاملة

28-26

SearchInform SIEM

31-29

SearchInform FileAuditor

كمية البيانات التي تخزنها الشركة في المتوسط تعتبر ضخمة. و تحتوي بعض هذه البيانات على معلومات سرية: بيانات شخصية و مالية، رسومات، و الأصول الرقمية الأخرى. ينبغي تخزين كل فئة من هذه البيانات الحساسة و معالجتها و توزيعها وفقا للقواعد المقابلة.

- البيانات الهامة متاحة دائمًا في متناول اليد.
- حماية الملفات في أي تطبيق.

SearchInform هي عبارة عن منصة حماية مركبة متعددة المستويات ضد مخاطر أمن المعلومات.

مستويات أمن المعلومات التي توفر فيها منتجات SearchInform الحماية لها:

المستوى الأول	المستوى الثاني	المستوى الثالث
حماية الملفات و التي يتم تنفيذها باستخدام FileAuditor أداة (DCAP)	يتضمن نظام DLP الحماية على مستوى محطات العمل و قنوات تناقل البيانات و المخاطر المتعلقة بالتعامل البشري.	نهج مركب في RiskMonitor يطبق حماية المخاطر و إدارة حماية البيانات.

تتكامل جميع الأنظمة بسلاسة و تعمل على قاعدة تكنولوجية واحدة و يمكن نشرها في غضون ساعات قليلة. يؤدي تكامل أي من الأنظمة إلى زيادة و توسيع الحماية بشكل أكبر.

البيانات الهامة متاحة دائمًا في متناول اليد.

SearchInform FileAuditor هو أحد حلول DCAP (Data-Centric Audit and Protection) للتدقيق و الحماية المرتكزان على البيانات) للتدقيق الآلي لتخزين المعلومات و البحث عن انتهاكات حق الوصول و تتبع التغيرات التي تم إجراؤها على البيانات الهامة. يحمي النظام المستندات السرية من الإجراءات الضارة للموظفين، سواء عن غير قصد أو عن قصد، كما يقوم بترتيب الأمور في نظام الملفات.

كيف يقوم FileAuditor بحل مشكلة مراقبة أمن المعلومات الهامة:

التدقيق في حقوق الوصول

يوفر حقوق الوصول إلى المعلومات (الوصول الكامل، التحرير، القراءة، الكتابة، القراءة والتغيير، إلخ). يتبع الموظفون الذين ليس لديهم حق الوصول المصرح به إلى البيانات، يُعثر على الملفات السرية المخزنة التي تقوم بانتهاك قواعد الأمان المعمول بها (في المجال العام، في مجلدات الشبكة المشتركة، على أجهزة كمبيوتر الموظفين، و ما إلى ذلك)

تصنيف البيانات المعرّضة للخطر

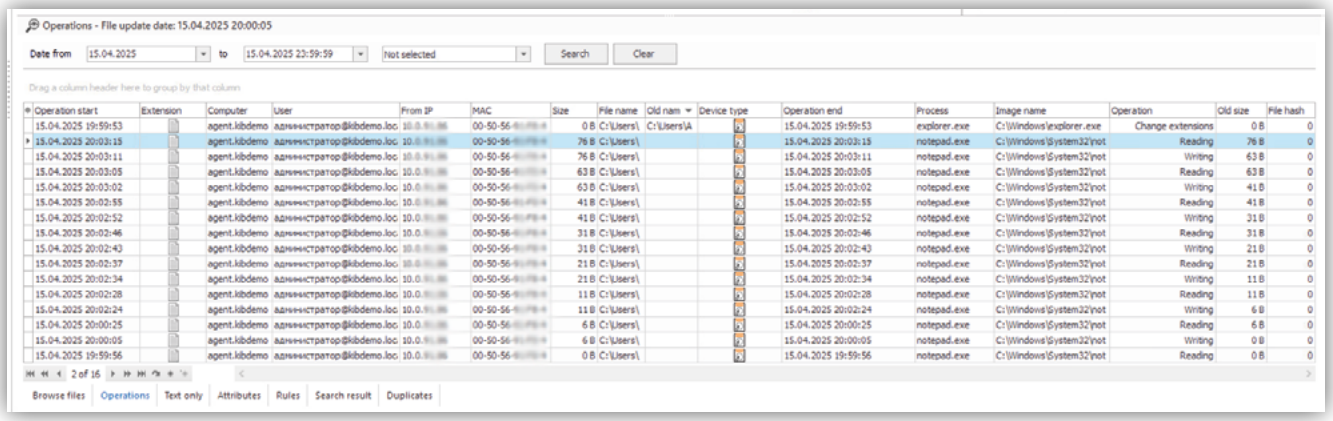
يبحث في تدفق المستندات عن الملفات التي تحتوي على معلومات مهمة، و يضيف علامات مخصصة لكل ملف، تشير العلامة المخصصة إلى نوع المعلومات التي يحتوي عليها الملف: البيانات الشخصية، و الأسرار التجارية، و أرقام بطاقات الائتمان، وما إلى ذلك.

مراقبة وحظر إجراءات المستخدم

يراجع عمليات المستخدم مع نظام الملفات. يدقق عمليات المستخدم مع نظام الملفات. يتوفر لدى موظفي أمن المعلومات دائمًا أحدث المعلومات حول دورة حياة الملف (الإنشاء و التحرير و النقل و الحذف، و ما إلى ذلك) في متناول اليد. يمنع الوصول إلى المستند و نقله في أي تطبيق.

أرشفة الوثائق الهامة

يقوم بعمل نسخ احتياطية من الملفات الهامة التي يتم العثور عليها على جهاز الكمبيوتر أو الخادم أو في مجلدات الشبكة، و يحفظ سجلات مراجعتها. تساعد أرشفة البيانات السرية في التحقيق في الحوادث و تضمن استعادة المعلومات المفقودة.



عمليات الملف في الوضع النشط (Active Mode: file activity monitoring)

كيف يعمل هذا النظام؟

يتم الاحتفاظ بالمعلومات التي تم جمعها في قاعدة البيانات، كما يتم الاحتفاظ بنسخ من الملفات الهامة. هذا يضمن بقاء المستندات متاحة حتى بعد الحذف.

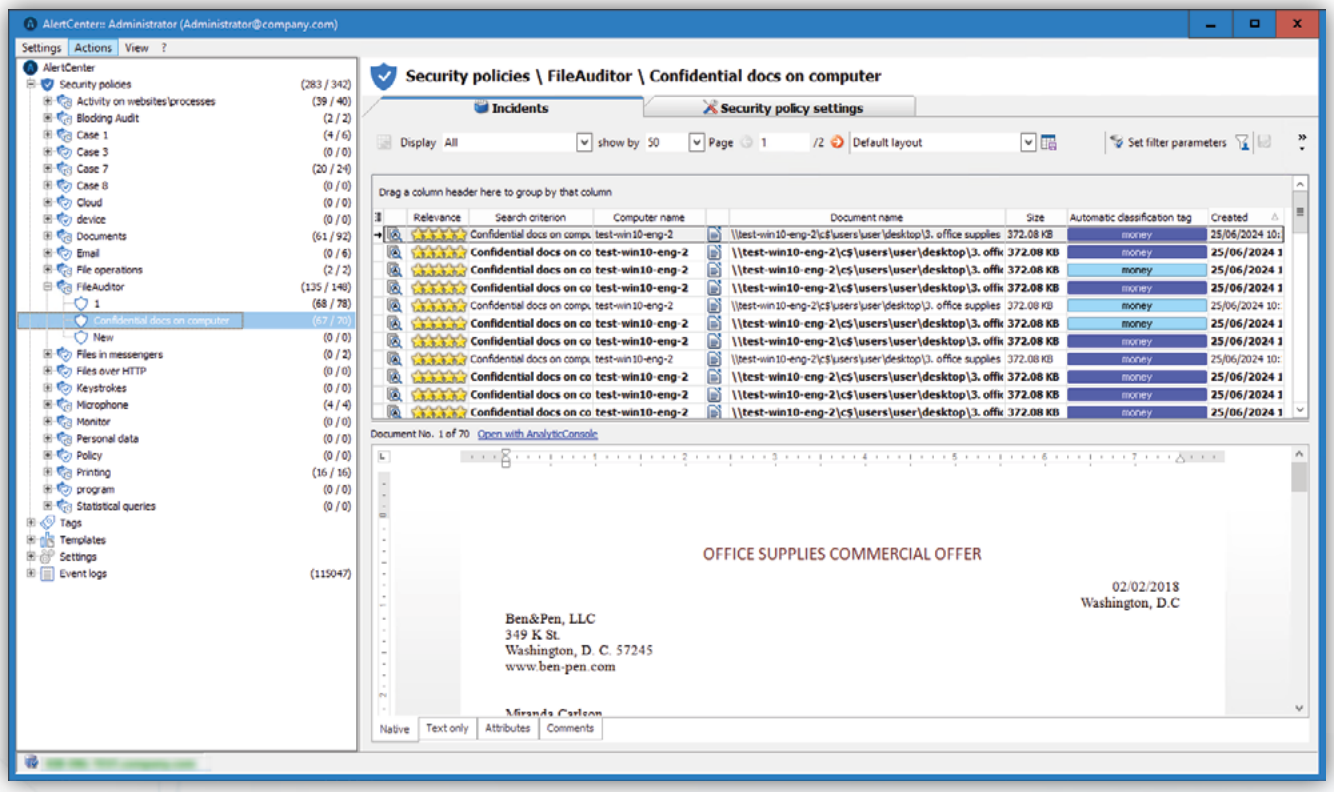
تحليل بيانات

الوحدة التحليلية لبرنامج FileAuditor تقوم بعرض نتائج عمليات مسح نظام الملفات استنادًا إلى قواعد محددة مسبقًا. تدعم إعدادات هذه القواعد أنواعًا متعددة من آليات البحث، و يمكن تقديم النتائج في شكل تقارير مرئية (مثل مصادر البيانات، و حقوق الوصول، و الأخطاء)، أو بصيغة شجرية تُبرز الهيكل الهرمي لنظام الملفات.

يعرض البرنامج ما يلي:

- بنية المجلدات مع توضيح صلاحيات المستخدمين لكل ملف أو مجلد، مما يتيح رؤية واضحة لمستوى الوصول عبر النظام.
- العمليات التي تتم على الملفات الحساسة، بما في ذلك تواريخ الإنشاء و التعديل، لرصد أي تغييرات غير مصرح بها.
- عدد الوثائق الحساسة الموجودة على القرص أو داخل مجلد معيّن، مع إمكانية تحديد نقاط التركّز أو المخاطر.
- تصنيف الملفات بحسب نوع البيانات (مثل اتفاقيات السرية، البيانات الشخصية، البيانات المالية)، ما يُسهّل عمليات المراقبة و الامتثال.

يمكن تكوين إشعارات انتهاك السياسات في AlertCenter. فعلى سبيل المثال، إذا حدد FileAuditor وجود ملف حساس على جهاز أحد المستخدمين دون امتلاكه الصلاحيات المناسبة للوصول إليه، فسيتم تلقائيًا إخطار أخصائي التخفيف من المخاطر المعين عبر البريد الإلكتروني.



AlertCenter

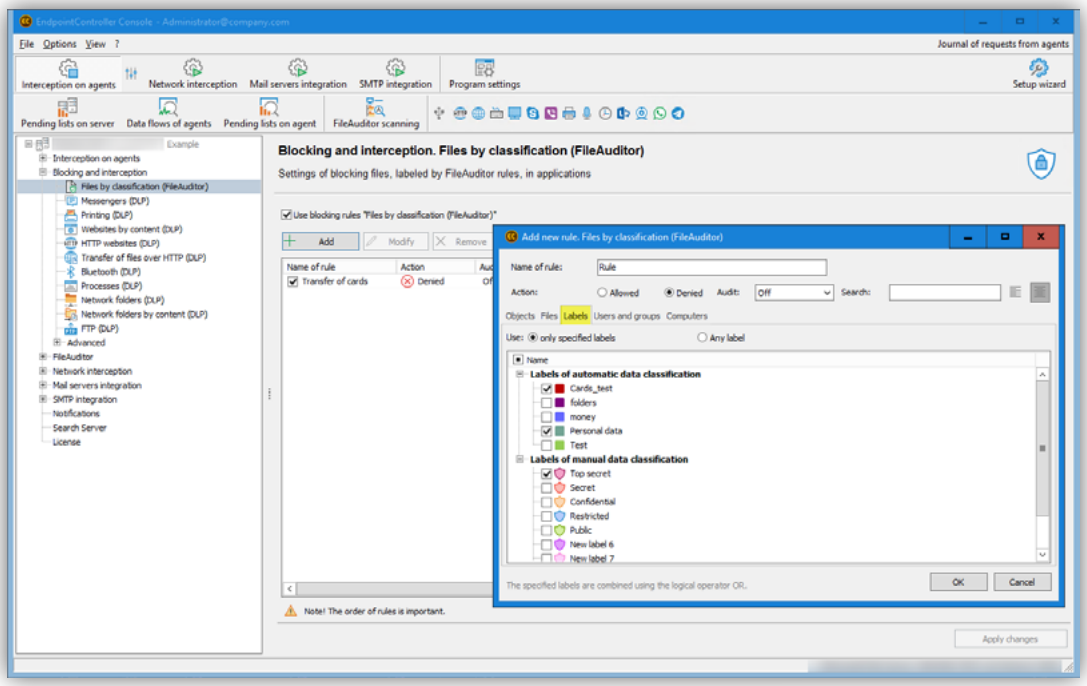
تُخزَّن المعلومات التي يتم جمعها بواسطة الوكلاء و وحدة فحص الشبكة في قاعدة بيانات تعمل على Microsoft SQL Server أو PostgreSQL، بينما تُحفَظ نسخ من الملفات الحرجة في المستودع. هذا يضمن بقاء المستندات متاحة حتى بعد حذفها.

حماية البيانات

تمنع آلية الحظر المبنية على المحتوى تنفيذ العمليات الخطرة على الملفات، بما في ذلك الإجراءات غير المصرح بها على المستندات ضمن مختلف التطبيقات، أو محاولات النقل المشبوهة، أو الوصول من قبل جهات غير مخوّلة.

تنطبق قواعد الحظر على الملفات المصنّفة تلقائيًا أو تلك التي يتم تصنيفها يدويًا. يقوم النظام بإسناد تسميات (Labels) استنادًا إلى نوع المعلومات – مثل "سر تجاري"، أو "بيانات شخصية"، أو "عقود".

يتم ضبط الصلاحيات و القيود وفقًا لتصنيف المعلومات، مما يحدّد بدقة من يُسمح لهم – من المستخدمين، أو الأجهزة، أو التطبيقات – بالتعامل مع كل فئة من فئات الملفات.



تعيين قواعد الحظر حسب التصنيفات في SearchInform FileAuditor

يتيح FileAuditor حظر الوصول إلى الملفات عبر أي تطبيق، بغض النظر عن نوعه أو إصداره أو مصدره. تُفرض القيود على مستوى نظام الملفات، حيث يتحكّم النظام في منح أو منع التطبيقات من قراءة البيانات. يُتيح هذا النهج فرض الرقابة الكاملة على عمليات قراءة و تعديل و تمرير المستندات التي تحتوي على معلومات سرّية، إلى جانب إمكانية ضبط إعدادات إضافية تتعلق بالوصول إلى الملفات، بما يتماشى مع سياسات الأمان المؤسسية.

المزايا

- يتم دمج حلول التحكم في الوصول إلى البيانات (DCAP) بسلاسة مع قدرات نظام منع فقدان البيانات (DLP).
- يمكن جدولة المراقبة أو تشغيلها تلقائيًا عند وقوع أحداث أو تحقق شروط معيّنة، مما يساهم في تقليل الضغط على الجهاز و توفير استهلاك الذاكرة. يمكن كذلك الاحتفاظ فقط بالوثائق الحساسة، و تساعد آلية إزالة التكرار في تقليل استخدام مساحة التخزين.
- يُمكن نشر البرنامج في بيئة سحابية، ما يتيح للشركات التي لا تمتلك بنية تحتية تقنية خاصة بها استخدام النظام و الاستفادة من قدراته دون الحاجة إلى استثمارات تقنية داخلية.
- تسمح إعدادات القواعد القابلة للتخصيص للمختصين بتجنّب المهام غير الضرورية و التركيز فقط على مراقبة البيانات الحساسة.
- يوفر النظام تتبعًا لحظيًا لتغييرات الملفات، حيث يحتفظ بعدد محدد من النسخ السابقة، مما يساعد في التحقيقات الداخلية.
- كما يوفّر حماية استباقية للملفات من خلال إمكانية حظر الوصول إلى المستندات لمنع التعديلات أو النقل غير المصرّح به.

SearchInform DLP

يحمي الشركة من تسرب المعلومات الحساسة، و يتحكم في البيانات الخاملة و البيانات المتحرّكة.

يراقب جميع قنوات نقل البيانات الشائعة، و يحلل المعلومات، و يكشف الانتهاكات و يمنعها، و يقدم التقارير إلى الشخص المسؤول.

تضمن SearchInform حماية فعّالة للبيانات أثناء النقل

احموا بيانات مؤسساتكم و استفيدوا من الميزات التالية:

- التحكم الكامل في قنوات نقل البيانات المُستخدمة في العمليات اليومية، لتفادي أي تسرب غير مقصود للمعلومات.
- مجموعة من الأدوات التحليلية الذكية، بما في ذلك التعرف الضوئي على الحروف (OCR)، و البحث عن المحتوى المتشابه، و البحث باستخدام الصور.
- أرشفة مفصلة للحوادث لدعم التدقيق و التحقيقات الشاملة.
- خيارات نشر مرنة، سواء على البنية التحتية الداخلية أو عبر السحابة، مع دعم كامل للتكامل مع Microsoft 365.

1. يراقب قنوات نقل البيانات الأكثر شيوعًا في الاتصالات المؤسسية.
2. يتحكّم في أدوات الوصول عن بُعد و أدوات العرض المرئي لضمان عدم إساءة استخدامها.
3. يفحص البيانات تلقائيًا وفقًا لسياسات الأمان المُعدّة مسبقًا.
4. يُخطر مسؤول أمن المعلومات و يمنع إرسال البيانات السرّية عند رصد حادث محتمل.
5. يرصد الأنشطة المشبوهة و الانحرافات داخل الشبكة و يصدر تنبيهات فورية.
6. ينشئ أرشيفًا للحوادث يحتوي على سجلات مفصلة لأنشطة المستخدمين.

امتثال كامل للمتطلبات التنظيمية

يساعد الحل على ضمان الالتزام المستمر بالمعايير و اللوائح داخل المؤسسة.

حماية شاملة للبيانات و الوقاية من التهديدات

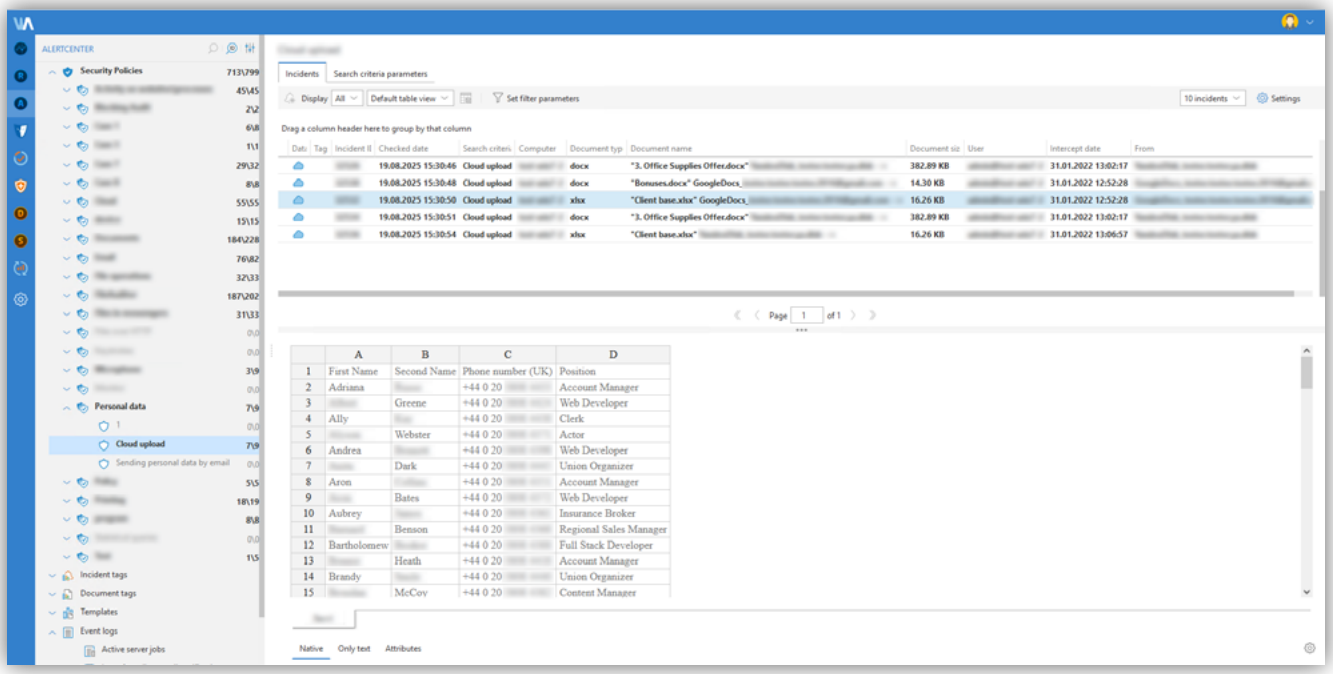
يقوم نظام SearchInform DLP بتحديد الثغرات في نقل البيانات و تحليلها، و يستخدم تحليلات متقدمة لربط التهديدات و كشفها بدقة.

حماية مستمرة لبياناتكم المؤسسية على مدار الساعة

يؤمّن الحل المعلومات بشكل دائم، بغضّ النظر عن أماكن تواجد الموظفين أو طبيعة بيئة العمل.

سياسات الأمان

يُقدّم النظام أكثر من 250 سياسة أمان جاهزة، تشمل سياسات عامة الاستخدام و أخرى مخصصة لقطاعات صناعية محددة. كما يُمكن إنشاء سياسات أمان مخصّصة وفقًا لاحتياجات المؤسسة.



السياسات الأمنية في Alert Center

المزايا

- **أعلى مستويات الحماية في سوق أنظمة DLP،**
  حيث يوفّر النظام منعًا لتسرب البيانات استنادًا إلى المحتوى، و ذلك عبر الرسائل و الملفات في تطبيقات المراسلة، و البريد الإلكتروني، و الخدمات السحابية، و سطح المكتب البعيد، و تصفّح الإنترنت، و الطباعة، و الأجهزة القابلة للإزالة.

- **دعم لمحطات العمل العاملة بأنظمة Windows / Linux / Mac،**
  بالإضافة إلى خوادم DLP لأنظمة Windows و Linux، مع قواعد بيانات MS SQL و PostgreSQL، تم تحسينها لتوفير كفاءة عالية في التخزين و التحليل.

- **أحدث تقنيات التحليل في السوق،**
  تتضمن أنماطًا تقليدية (أكثر من 430 نمطًا افتراضيًا)، و خوارزميات ذكية، و تعلّم الآلة، و تحليلات سلوكية متقدمة.

- **لا يقتصر الحل على الحظر فقط،**
  بل يتيح أيضًا معالجة البيانات مثل التشفير، و العزل (Quarantine)، و إرجاع الرسائل إلى المُرسل.

- **يوفّر نظام DLP تقنيات فريدة من نوعها مثل Automated Profiling،**
  الذي يتيح تقييم المخاطر المرتبطة بالعامل البشري، بل و يدعم أيضًا اتخاذ قرارات إدارية مناسبة بناءً على هذا التقييم.

SearchInform Risk Monitor

توفر SearchInform مقاربة شاملة للمراقبة الداخلية، من خلال توسيع نطاق حلول DLP و دمج مفهومين قويين: الوقاية من الحوادث و الحد من التهديدات الداخلية.

يعمل نظام Risk Monitor على حماية أعمالكم من الخسائر المالية و الأضرار التي تمس السمعة الناتجة عن التهديدات الداخلية.

حل SearchInform متاح للتنفيذ محليًا أو عبر البيئة السحابية

لا تحتاج الشركات إلى المفاضلة بين الأمان و سهولة الاستخدام و التكلفة، إذ يمكن نشر الحل في البيئة السحابية دون الحاجة إلى أجهزة مخصصة. يقوم Risk Monitor بجمع البيانات و معالجتها و تخزينها ضمن بيئة افتراضية بالكامل.

يُعد هذا النموذج من النشر مثاليًا للشركات التي لا تمتلك بنية تحتية تقنية خاصة بها، أو التي تنتشر مكاتبها في مدن مختلفة، أو التي تضم عددًا كبيرًا من الموظفين العاملين عن بُعد.

منصة شاملة لإدارة المخاطر تعتمد على وكيل واحد.

أمن مرتكز على المستخدم

- يُسهم في رفع إنتاجية الموظفين من خلال تقليل المخاطر المرتبطة بسلوكيات العمل غير الآمنة.
- يُوفّر حماية فعّالة ضد المخاطر البشرية داخل المؤسسة، و يُساعد على توقّع أنماط سلوك الموظفين قبل أن تتحول إلى تهديدات.
- يُساعد الإدارة في تعزيز ولاء الفرق و تحسين بيئة العمل من خلال فهم أعمق للسلوك الوظيفي.
- يُتيح مراقبة و تقييم العامل البشري كجزء من منظومة أمن المعلومات الشاملة.

تسهيل الامتثال التنظيمي

- يُسهم في حل مشكلات الامتثال للمتطلبات التنظيمية و المعايير القانونية بفعالية.
- يُجري تحقيقات رقمية جنائية و تحليلات استعادية لدعم التدقيق و اكتشاف الحوادث بعد و قوعها.

أمن مرتكز على البيانات

- يُخفّف من مخاطر تسرب البيانات عبر الرقابة الدقيقة على المعلومات الحساسة أينما وُ جدت.
- يوفّر حماية مخصصة للبيانات الحساسة المخزّنة على أجهزة المؤسسة، بغضّ النظر عن مكان المستخدم أو طبيعة الجهاز.

الحل المتقدّم

- يكتشف حوادث التلاعب الداخلية الخبيثة، بما في ذلك الاحتيال المؤسسي و استغلال الموارد لتحقيق مكاسب شخصية.
- يسهّل عمليات الامتثال التنظيمي و يساعد في إجراءات التحقيق و التحليل بأدوات دقيقة و موثوقة.
- يراقب العامل البشري ويتنبأ بالمخاطر المرتبطة بالموارد البشرية، مما يتيح تدخلًا استباقيًا قبل حدوث الانتهاكات.
- يعمل كنظام إنذار مبكر، يكتشف التهديدات المحتملة أو الظروف التي قد تؤدي إلى خروقات، و يصدر تنبيهات فورية عند رصد المخاطر.

يوفّر Risk Monitor مجموعة أدوات قوية و آلية لمراقبة الموظفين، و تقييم المخاطر، و إجراء التدقيقات الداخلية.

يساعد هذا النظام على ضمان توافق سياسات شركتك مع المتطلبات التنظيمية ذات الصلة، كما يُمكّنك من تقييم مدى مواءمة تدابير الأمان المعتمدة مع أحدث المعايير الصناعية.

القدرات

يجمع معلومات مفصلة حول أنشطة المستخدم للتعامل مع الانتهاكات خطوة بخطوة.

ينشئ أرشيفًا للمعلومات التي تم اعتراضها، مما يسهل امتثال المنظمين و يعزز سياسات الأمان الضرورية لتقليل المخاطر.

ينبه إلى وجود تهديد محتمل قبل و قوع أي حادث، و بالتالي تعزيز ثقافة أمن الشركات وزيادة الوعي بالمخاطر الداخلية.

يؤمّن الحماية للشركة من المخاطر التي قد يسببها الموظفون، و يتنبأ بأنماط سلوك الموظفين.

يساعد على زيادة إنتاجية الموظفين و يساعد في إدارة ولاء الفريق.

التقاط المعلومات

يضمن حل SearchInform حماية جميع قنوات نقل البيانات الشائعة الاستخدام.

E-mail

جمع الرسائل الإلكترونية، و تصنيفها، و عزلها (Quarantine). يوفّر الحماية لكل من البريد الإلكتروني المؤسسي و العام (مثل Gmail و غيره). كما يقدّم الحماية لعملاء البريد الإلكتروني الذين يستخدمون البروتوكولات الكلاسيكية مثل IMAP، SMTP، MAPI، بالإضافة إلى حماية البريد الإلكتروني عبر المتصفح.

Monitor+Keylogger

يلتقط لقطات شاشة و يسجل شاشة المستخدم بالكامل، بما في ذلك أنشطة البرامج و التطبيقات. كما يُمكنه التقاط صور أو فيديو عبر كاميرا الويب، و تسجيل ضغطات لوحة المفاتيح (Keylogging)، و اكتشاف محاولات تصوير الشاشة باستخدام الأجهزة المحمولة. يدعم النظام أيضًا التعرّف البيومتري على المستخدمين من خلال تقنية التعرّف على الوجه.

IM

جمع، وتصنيف، وحظر الرسائل و المكالمات و الملفات المُرسلة عبر منصات المراسلة، سواء المؤسسية أو المتاحة للعامة، بما في ذلك WhatsApp و Telegram.

Connected devices

جمع و تصنيف و حظر و تشفير إجباري للملفات التي يتم نقلها عبر منافذ الإدخال/الإخراج الخاصة بأجهزة تخزين البيانات.

Software

يتتبّع الوقت المُستغرق في التطبيقات و المتصفحات، و يُقيّم الإنتاجية، و يُحلّل نشاط المستخدمين أثناء التحقيقات المؤسسية.

Cloud services

جمع و تصنيف و حظر الملفات المُرسلة إلى الخدمات السحابية أو برامج التعاون (مثل Zoom).

Microphone

يستخدم النظام التحويل التلقائي للنصوص الصوتية كجزء من آلية مراقبة الامتثال الأمني.

HTTP

تتولى هذه الوحدة جمع و تصنيف و حظر أي حركة مرور عبر المتصفح لا يتم التقاطها بواسطة وحدات التحكّم الأخرى.

FTP

جمع وتصنيف و حظر حركة مرور بروتوكول نقل الملفات (FTP).

Print

جمع و تصنيف و حظر الملفات المُرسلة للطباعة.

مركز التحكّم

DataCenter

يتولى إدارة فهارس النظام و قواعد البيانات، و يراقب سلامة النظام للتأكد من استقراره، كما يضمن الاتصال بالأنظمة الخارجية مثل Active Directory و SOC و خادم البريد الصادر. تتم إدارة صلاحيات وصول المستخدمين من خلال مركز البيانات (DataCenter).

AlertCenter

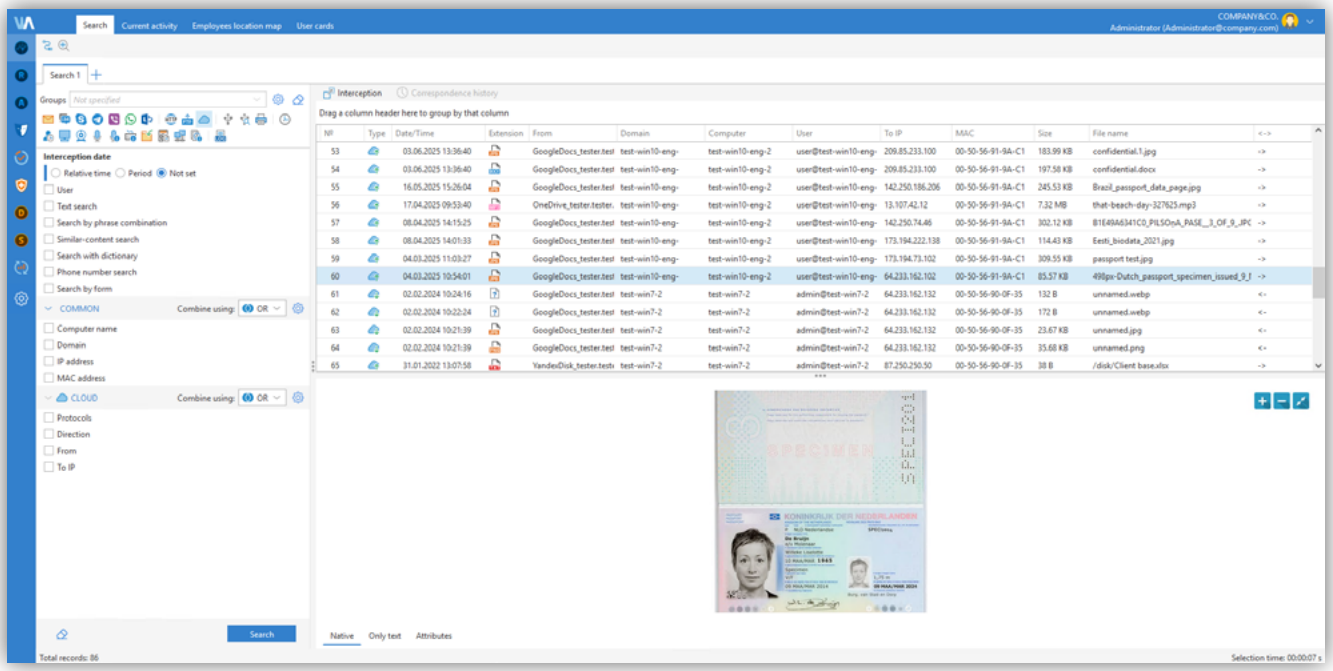
تُعدّ هذه الوحدة بمثابة "العقل المفكر" للنظام، حيث يتم إعداد سياسات الأمان. تتضمن أكثر من 250 سياسة أمان مُعدة مسبقًا قابلة للتعديل. كما يتيح النظام إنشاء قواعد مخصصة لفحص البيانات التي تم اعتراضها و حظرها، بالإضافة إلى إمكانية ضبط جداول الفحص و إرسال إشعارات تلقائية عند تحقق الشروط المحددة.

يمكن لأخصائيي الأمن الاطلاع على تقارير الحوادث عبر وحدة AlertCenter على محطة عملهم، أو من خلال واجهة الويب المتاحة عبر الحاسوب المحمول أو الجهاز اللوحي أو الهاتف الذكي.

AnalyticConsole

تُستخدم وحدة التحليل لفحص البيانات التي تم اعتراضها و مراقبة أنشطة المستخدمين. و توفّر خوارزميات بحث متعددة و نماذج تقارير جاهزة تُسهّل عمل المختصين و تحليلهم للحوادث.

جميع ميزات مركز التنبيهات (AlertCenter) و وحدة التحليل (AnalyticConsole) متاحة عبر واجهة ويب، مما يُمكّن أخصائيي الأمن من الاستجابة السريعة للتنبيهات و اتخاذ إجراءات فورية ضد التهديدات المحتملة.



وحدة البحث (Search Module) في وحدة تحكم الويب الخاصة (Web Console) بـ SearchInform Risk Monitor

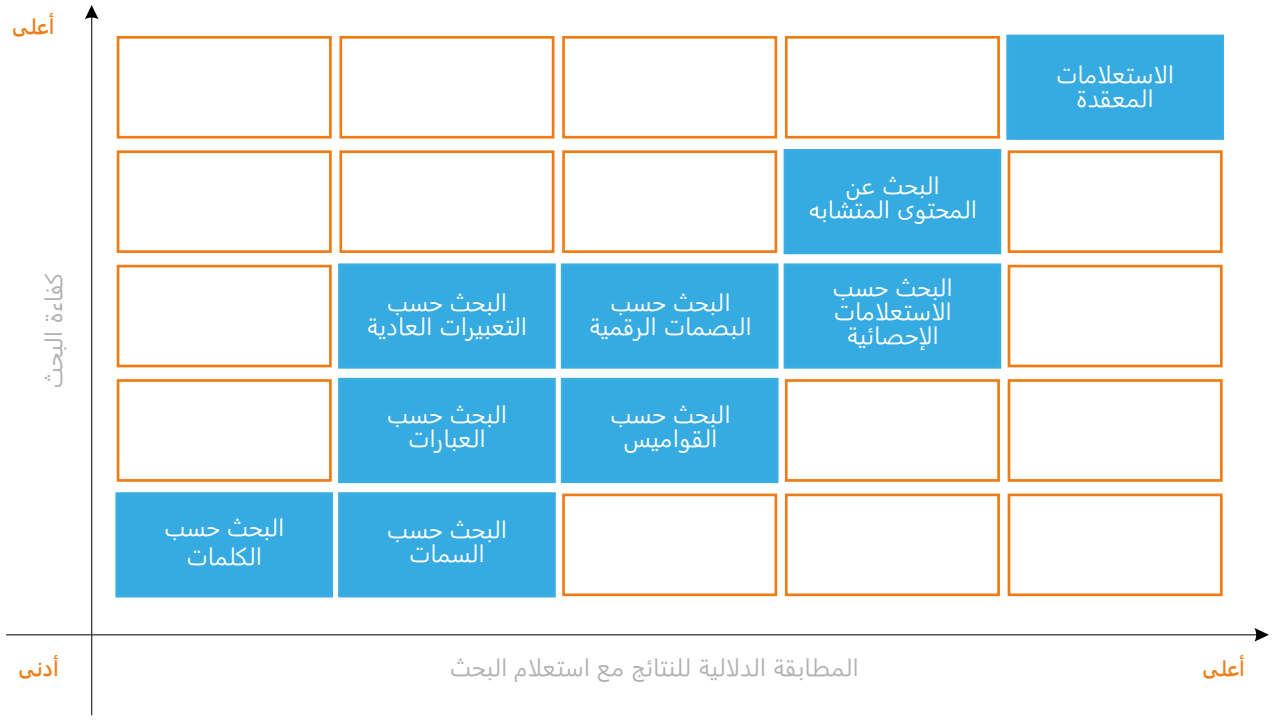
القدرات التحليلية

لرفع كفاءتهم، يحتاج أخصائيو أمن المعلومات إلى قدرات تحكّم شاملة عبر جميع قنوات الاتصال، إلى جانب وظائف متقدّمة للبحث في البيانات التي تم اعتراضها وتحليلها.

تُتيح الوحدة التحليلية القوية، مع خيارات البحث المتنوعة و تقنيات التحليل التلقائي للرسوميات و الصوتيات، لأخصائي واحد فقط أن يُشرف على أعمال آلاف الموظفين بدقة و كفاءة عالية.

تحليل المحتوى النصي

توفّر تقنيات البحث الفريدة، مثل البحث عن المحتوى المماثل و الاستعلامات المعقدة، تحليلاً معمقًا للرسائل النصية و المستندات. فعلى سبيل المثال، يستطيع خوارزم البحث عن المحتوى المماثل تحديد السجلات السرية حتى و إن تم تعديلها، حيث يبحث في الملفات التي تتشابه دلاليًا مع الاستعلام و ليس فقط من حيث التطابق التقني. أما الاستعلامات المعقدة فتجمع بين عدة خوارزميات للبحث، و تربط الاستعلامات البسيطة باستخدام العوامل المنطقية مثل AND و OR و NOT.



تحليل المحتوى الرسومي

يعمل النظام على تحديد أنواع الصور المتداولة داخل الشركة – مثل ملفات PDF، الصور الفوتوغرافية، أو النسخ الممسوحة ضوئيًا – و يقوم بتصنيف ملفات الصور وفقًا لذلك. تقوم منظومة التعرف البصري على الحروف (OCR) المدمجة بتحديد المستندات التي تتطابق مع أنماط محددة، مثل جوازات السفر، البطاقات المصرفية، رُخص القيادة، و غيرها. تُتيح هذه التقنية للنظام اكتشاف البيانات الشخصية و المالية و أي بيانات حساسة أخرى ضمن الأرشيف، حتى و إن تم نقلها في هيئة مستندات ممسوحة ضوئيًا.

تحليل المحتوى الصوتي

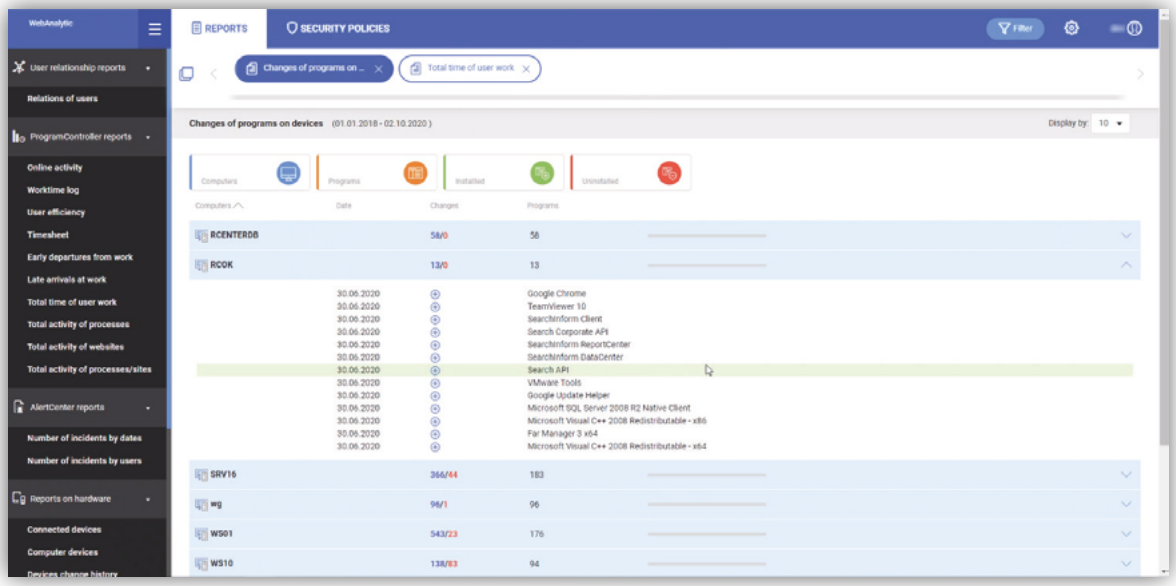
يقوم حل SearchInform بتحويل التسجيلات الصوتية إلى نصوص مكتوبة، ثم يتحقّق مما إذا كانت النصوص الناتجة متوافقة مع سياسات الأمان المُعتمدة. يوفّر النظام خيار تفعيل تحليل الصوت تلقائيًا عند اكتشاف كلام منطوق، أو عند تشغيل عمليات أو برامج محددة تم تعريفها ضمن سياسة الأمان ذات الصلة.

التقارير وتحليل السلوكيات (UEBA)

يقوم Risk Monitor بعرض جميع الأحداث والارتباطات داخل الشركة بشكل مرئي على هيئة تقارير، يمكن الوصول إليها من خلال وحدة التحليل (Analytic Console) أو واجهة الويب. يوفّر النظام بشكل افتراضي أكثر من 30 نموذجًا أساسيًا للتقارير الجاهزة للاستخدام. كما يُمكن استخدام معالج إنشاء التقارير لتصميم تقارير مخصصة بالكامل دون أي قيود على معايير البحث أو التصفية.

تقرير البرامج والأجهزة

يقوم الحل برصد أي تغييرات تطرأ على الأجهزة المثبّتة أو الأجهزة المتصلة، مما يُسهم في إدارة الأصول بفعالية ويمنع حالات السرقة أو الاستبدال غير المصرّح به للمعدات. كما يقوم Risk Monitor بتسجيل تقارير حول تثبيت البرامج أو إزالتها، لضمان الرقابة المستمرة على البيئة البرمجية داخل المؤسسة.

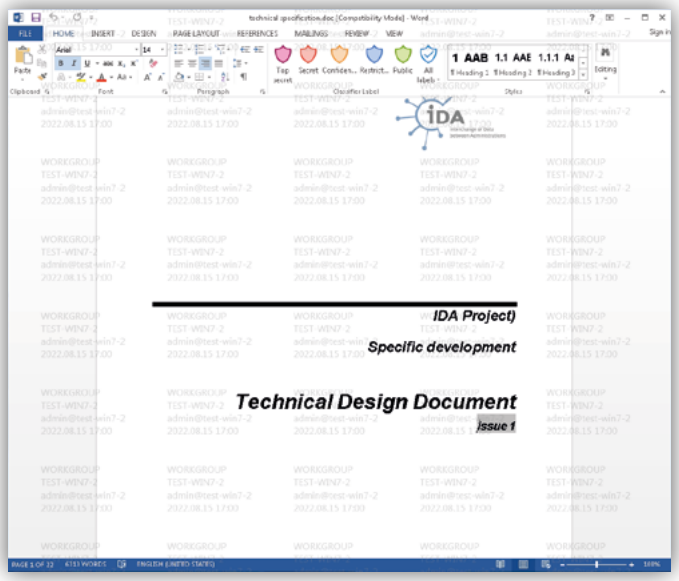


تقرير البرامج و الأجهزة (Software and hardware report)

التحقيقات و التحكّم

اكتشاف تسرب البيانات عند إخراجها عبر لقطات الشاشة أو صور الشاشة.

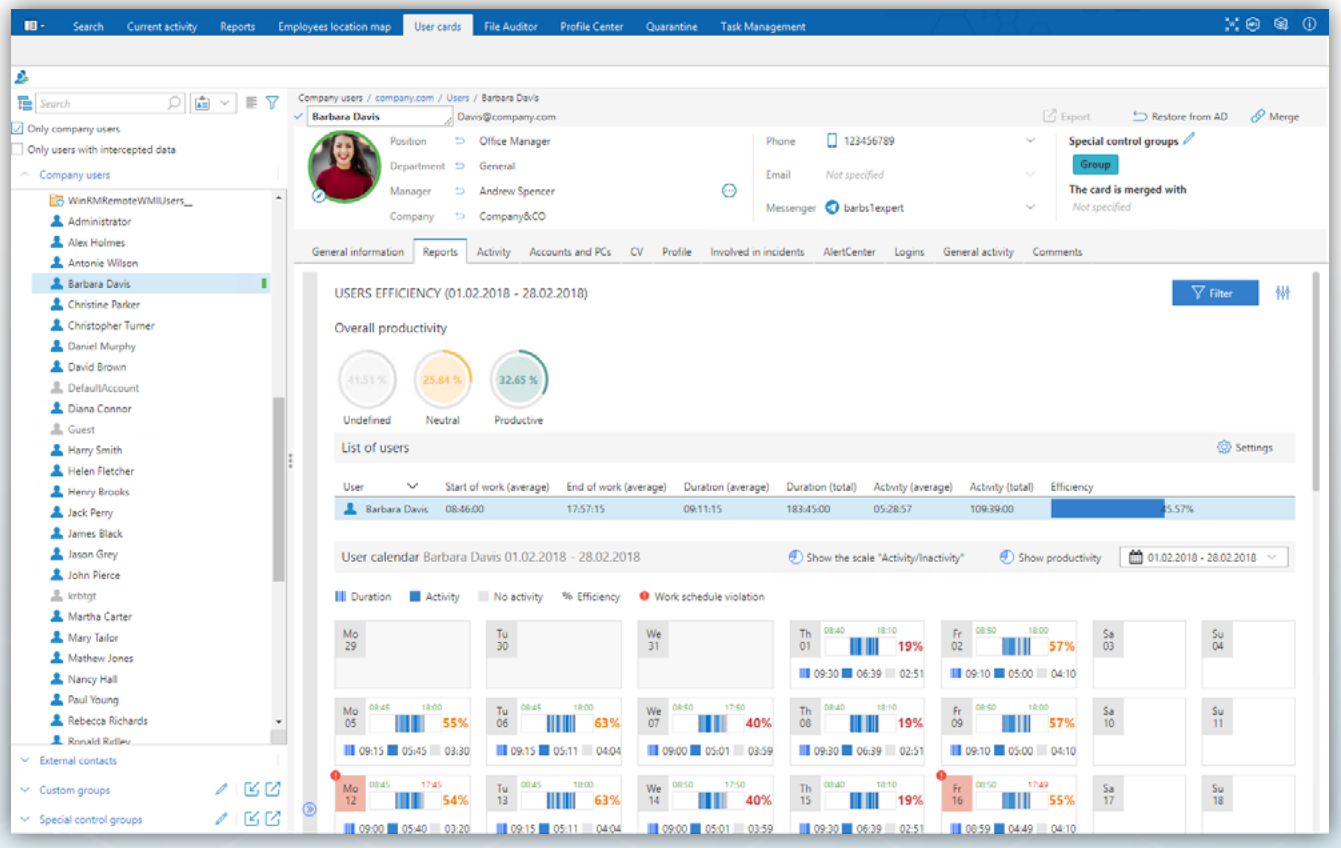
يُعدّ تحديد مصدر تسرّب البيانات عند قيام المستخدم بالتقاط لقطات شاشة أو تصوير الشاشة أمرًا بالغ الصعوبة. إلّا أن أداة العلامات المائية (Watermarking) المدمجة في SearchInform Risk Monitor تُعالج هذه المشكلة بفعالية. من خلال تحليل لقطة شاشة أو صورة ملتقطة من محطة عمل محمية تم العثور عليها خارج بيئة المؤسسة، يمكن لمختص أمن المعلومات تحديد مصدر تسرّب البيانات بسهولة، و ذلك عبر العلامة المائية الظاهرة على الشاشة. تتضمّن العلامة المائية معلومات عن الجهاز و الموظف الذي يعمل عليه، مما يتيح تتبّع مصدر التسريب بدقّة، حتى في الحالات التي يتم فيها إخراج البيانات بطرق غير تقليدية.



العلامات المائية المدمجة في Risk Monitor

بطاقات المستخدمين

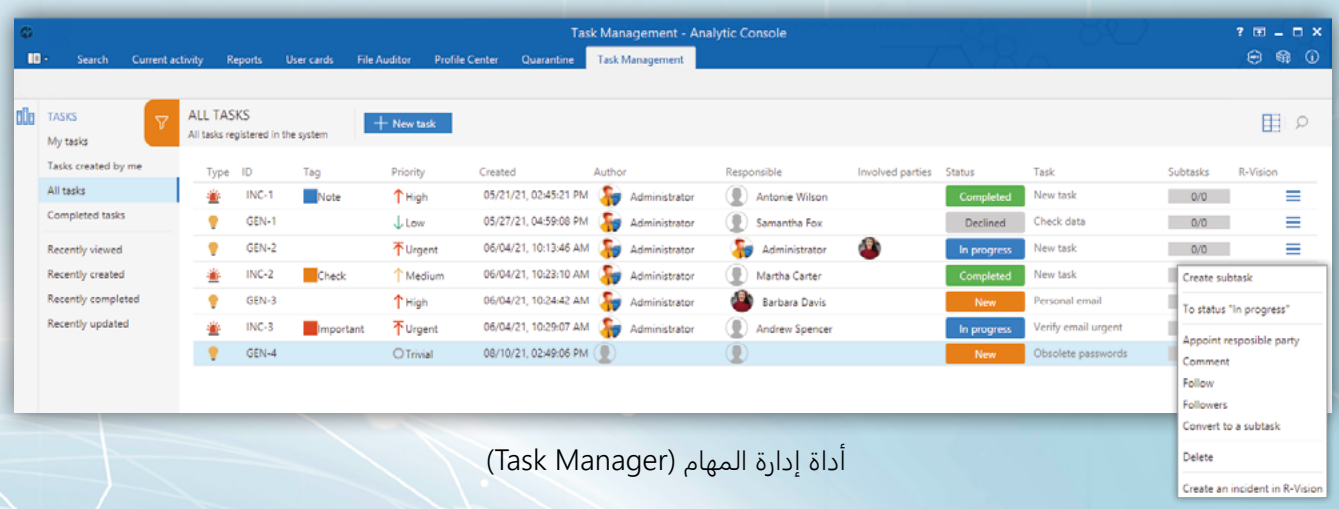
تقوم بطاقة المستخدم بجمع "ملف شخصي متكامل" لكل موظف، بحيث تُدرج تلقائيًا جميع الحوادث التي كان طرفًا فيها. تتضمّن البطاقة تقارير فردية، و معلومات السيرة الذاتية و بيانات الاتصال، إضافةً إلى تاريخ الوظيفة و المسار المهني للموظف.



بطاقات المستخدمين

إدارة التحقيقات

يساعد Task Manager أخصائيي أمن المعلومات في تنسيق المهام الأمنية، حيث يُتيح لهم توزيع المهام، و تتبع تقدم التحقيقات، و إعداد تقارير بالنتائج، بما في ذلك إمكانية تحويلها إلى مركز العمليات الأمنية (SOC).



أداة إدارة المهام (Task Manager)

الميزات الفريدة

1 ميزات تحليلية فريدة غير متوفّرة في أي أداة أخرى

إضافة إلى الميزات التحليلية التقليدية، مثل البحث باستخدام الماوس و التعبيرات العادية و بصمات الملفات النصية و OCR، يتيح SearchInform Risk Monitor ميزاتٍ تشابه بصمات مثل البحث عن صور مشابهة للصور الأصلية، و البحث حسب المحتوى في تسجيلات الفيديو لإجراءات المستخدم، مما يسمح لك بالتحقق فقط من الإجراءات محل الاهتمام.

2 أدوات تحقيق عالية الجودة في حل واحد

يتيح المنتج تسجيل صوت كلام المستخدم و إنشاء فيديو لإجراءات المستخدم، و تسجيل جميع أنواع عمليات المستخدم مع الملفات و المجلدات، و سجلات التدقيق، و الأجهزة، و البرامج. فضلًا عن مراقبة المخالفين عبر قنوات الصوت و الفيديو في الوقت الفعلي.

3 التحكم في كفاءة عمل المستخدم

تقوم أداة SearchInform Risk Monitor بتقييم كفاءة عمل المستخدم تلقائيًا في مختلف التطبيقات و على مواقع الويب، و تساعد هذه الوظيفة على تعزيز الانضباط في الشركة و اكتشاف المشكلات الحالية في العمليات التجارية.

4 استقرار النظام تحت الأحمال، و هو ما تؤكده الممارسة

من بين عملاء SearchInform، هناك مؤسسات كبيرة الحجم من مختلف المجالات التجارية، و ما يثبت هذه الحقيقة أن النظام يعمل بشكل مستقر على بيانات تكنولوجيا المعلومات المختلفة و تحت حمولة عالية.

5 إمكانية توسيع الوظائف مع المنتجات من نفس الشركة المصنعة.

تقدم SearchInform مجموعة من المنتجات، بما في ذلك Risk Monitor و DLP و SIEM و FileAuditor. تعمل جميع الأنظمة على نفس القاعدة التكنولوجية، و يتم دمجها بسلاسة و نشرها في غضون ساعات قليلة.

6 منصة مشتركة و يمكن الوصول إليها من أي جهاز

يمكن تقديم واجهة مستخدم SearchInform Risk Monitor بطريقتين – كعميل Windows و كإصدار ويب.

المزايا

وحدة تحليل قوية

توفر حلولًا سريعة ومرنة لإعداد التنبيهات و تحليل تدفّقات البيانات دون الحاجة إلى توظيف مختصين خارجيين. و بفضل منتجات SearchInform، يمكن لمختص واحد فقط الإشراف على عمل عدة آلاف من الموظفين بكفاءة عالية.

حماية استباقية من الحوادث

يوفّر Risk Monitor آلية ذكية لحظر المحتوى على جميع القنوات الخاضعة للرقابة، بما يضمن منع المستخدمين من نقل الملفات أو الرسائل التي تحتوي على معلومات سرّية. كما يقوم Agent بإخطار المستخدمين تلقائيًا عند حدوث انتهاك عرضي لسياسات الأمان، مما يُسهم في تعزيز ثقافة أمن المعلومات داخل المؤسسة.

التحكّم في الوصول عن بُعد

يوفّر حل SearchInform حماية شاملة للبيانات المنقولة عبر البيئات الافتراضية و أدوات الوصول عن بُعد. يتم تنفيذ المراقبة على عدة مستويات: مستوى الحافظة (Clipboard)، و أثناء الاتصال بأجهزة التخزين الافتراضية، و كذلك على مستوى الوظائف المحددة داخل البرامج (مثل عمليات النقل عبر قائمة السياق في TeamViewer).

قسم التنفيذ ومركز التدريب

تُمكّننا خبرتنا العملية مع أكثر من 4,000 شركة تعمل في مختلف القطاعات من تصميم مجموعات فريدة من سياسات الأمان بشكل سريع، بما يراعي المهام ذات الصلة و طبيعة نشاط العميل على وجه الخصوص.

سهولة النشر دون الحاجة إلى تغيير في بنية الشبكة

سيتمكّن مختصو تكنولوجيا المعلومات لدى العميل من تثبيت حل SearchInform خلال بضع ساعات فقط. ولا يؤثر إجراء التثبيت على سير عمل أنظمة المعلومات المحلية الخاصة بالشركة أو يعيق تشغيلها.

أدوات التحقيق في الحوادث

تساعد أدوات مراقبة الأنشطة عبر الإنترنت – مثل تسجيل المحادثات، و التقاط محتوى الشاشة في الوقت الفعلي، و مراقبة ضغطات لوحة المفاتيح، و تصوير الفيديو عبر كاميرا الويب، و إنشاء تدفقات معلومات و رسوم بيانية للاتصالات – في إعادة بناء الحوادث الأمنية خطوة بخطوة. كما يُعزّز Task Manager و أدوات البحث الآلي عن الحوادث من كفاءة فرق أمن المعلومات و أدائهم، مما يتيح الاستجابة بشكل أسرع و أكثر دقة.

الذكاء الاصطناعي (AI)

يقوم النظام تلقائيًا بالتعرّف على المستخدمين و التأكد مما إذا كان الحاسوب يُدار من قِبل مالكه الشرعي.و يتمكّن Risk Monitor من اكتشاف محاولات تصوير شاشة الحاسوب باستخدام الهواتف الذكية، كما يترك آثارًا رقمية مميزة عبر تطبيق علامات مائية فريدة تساعد في تحديد مصدر أي خرق محتمل للبيانات.

نموذج النشر السحابي

يمكن نشر جميع مكوّنات Risk Monitor في البيئة السحابية (سواء على سحابة SearchInform أو أي خدمة سحابية أخرى من طرف ثالث) دون التأثير على وظائف النظام أو أدائه. و يُعد هذا الأسلوب في النشر موفّرًا للتكلفة و فعّالًا من حيث الوقت، مما يتيح للمؤسسات الاستفادة من الحل بسرعة و مرونة عالية.

التكامل مع منتجات SearchInform الأخرى

يتكامل حل SearchInform بسلاسة مع كل من SIEM و FileAuditor، مما يعزّز مستوى أمن المعلومات و الوعي بالمخاطر داخل المؤسسة، و يُسهم في تقليل زمن الاستجابة للحوادث، كما يتيح التحقيق الكامل في الانتهاكات و معالجتها بفعالية.

SearchInform TimeInformer

ليس كل وجود للموظف في مكان العمل يعني بالضرورة انشغاله بمهامه المباشرة. فهناك دائمًا بعض غير المسؤولين الذين يكثرون من أخذ استراحات التدخين أو القهوة، والانشغال بـ أحاديث جانبية مع الزملاء، أو قضاء الوقت على شبكات التواصل الاجتماعي، أو التأخر عن الحضور إلى العمل، أو المغادرة مبكرًا.

نشاط الفريق

يُعد TimeInformer حلاً لمراقبة الموظفين يوفّر حماية للشركات من العمل غير الفعّال و الخسائر المالية المرتبطة بالعنصر البشري.

يقوم TimeInformer بفحص حواسيب الشركة ليساعدكم على تحديد ما يلي:

- مخالفو انضباط العمل الذين يتأخرون عن الحضور، أو يغادرون مبكرًا، أو يكثرون من أخذ استراحات التدخين و القهوة.
- المتكاسلون الذين ينشغلون بالأحاديث الجانبية، أو بالتسوّق عبر الإنترنت، أو يتشتتون بالألعاب و أنشطة أخرى.
- المستقلون الذين يؤدّون أعمالًا جانبية خلال الساعات المدفوعة من قبل الشركة.
- الموظفون غير الراضين الذين يؤثرون على زملائهم ضد صاحب العمل، أو الذين أصابهم الإرهاق بسبب ضغط العمل الشديد أو تكرار المهام المملة.

يقوم TimeInformer بمراقبة أوقات خمول الموظفين و أوقات عملهم، و يجمع البيانات حول البرامج التي يستخدمونها خلال اليوم. كما يُسجّل جميع المواقع التي يزورونها و يُصنّفها في مجموعات مختلفة مثل مواقع المواعدة، التسوّق الإلكتروني، الأخبار، و برامج التلفاز. تُستخدم هذه المعلومات لاحقًا لتقييم الإنتاجية الفعلية للموظفين استنادًا إلى معايير محددة مسبقًا.

التحكّم في الوقت الفعلي

لا يعمل TimeInformer في الخلفية فقط، بل يوفّر أيضًا عدة أوضاع نشطة. يتصل البرنامج بشاشات الحواسيب و الميكروفونات، مما يتيح لك متابعة الأنشطة على محطات عمل الموظفين في الوقت الفعلي.

يقوم بتحليل المفاوضات المهمة مع الشركاء و العملاء الرئيسيين، حيث يلتقط كلًا من الصوت و نشاط الشاشة في الزمن الحقيقي. كما يتيح الحل المراقبة المباشرة لما يصل إلى 16 شاشة موظف في وقت واحد.

و يمكن نشر TimeInformer في البيئة السحابية، مما يمنحك و صولًا كاملًا إلى جميع إمكانياته دون الحاجة إلى شراء أو صيانة أجهزة إضافية.

المساعدة في اتخاذ القرارات الإدارية

توفّر 33 تقريرًا مُعدًّا مسبقًا في TimeInformer بداية سلسة، و تمكّن من الكشف السريع عن غير المنتجين، و تساعد في تحسين سير العمل، و تنظيم الفرق، و ضمان تحقيق الأهداف.

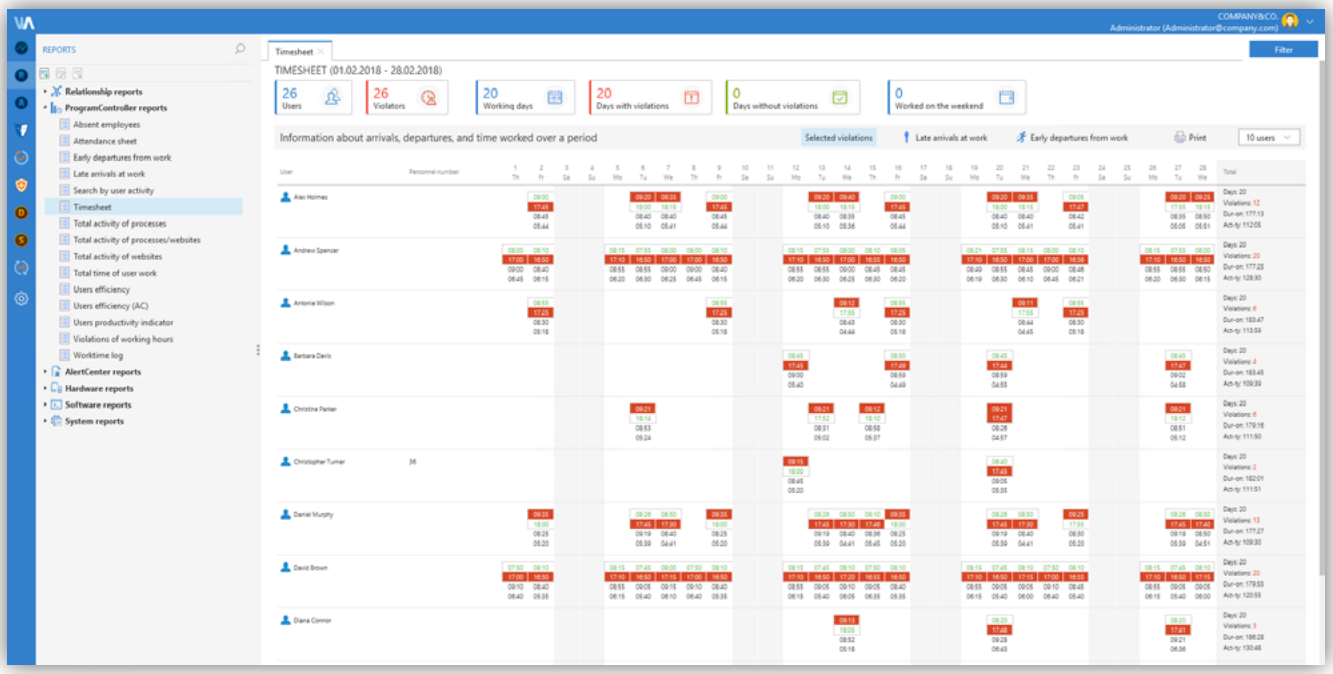
يقدّم TimeInformer المجموعات التالية من التقارير:

- تقارير حول نشاط المستخدم في التطبيقات و على مواقع الإنترنت
- تقارير حول البرامج، بما في ذلك سجل تثبيت البرامج و إزالتها
- تقارير حول الأجهزة، مع بيانات عن المعدات المثبّتة على الحاسوب و التغييرات التي طرأت على إعداداتها

يمكن تخصيص التقارير و الإشعارات بسهولة، حيث يقوم النظام بإخطار المسؤولين تلقائيًا عند حدوث أي انتهاك لسياسات الأمان.

واجهة سهلة الاستخدام

تتيح واجهة الويب للمديرين الإشراف على الموظفين من أي مكان في العالم. و يتم تخصيص الوصول إلى التقارير و الوظائف الإدارية وفقًا للأدوار و المسؤوليات. كما تُرسل تنبيهات تلقائية عبر البريد الإلكتروني لإخطار المسؤولين بأي نشاط مشبوه من قِبل الموظفين.



جدول الدوام في واجهة الويب (Timesheet in the web interface)

المزايا

- محمي من الحذف و مهيّأ لإرسال تنبيه عند محاولة الحذف.
- واجهة ويب تتيح الوصول إلى نتائج المراقبة من خارج المكتب.
- تكامل مع منتجات SearchInform، مما يساعد على إجراء التحقيقات الداخلية بكفاءة.
- مراقبة أنشطة المستخدمين حتى عند عملهم من المنزل أو أثناء رحلات العمل.

خدمات الأمن المُدارة من SearchInform

توفّر خدمات الأمن المُدارة (MSS) من SearchInform حماية مستمرة للبيانات الحساسة، وتُسهم في تحسين كفاءة الأعمال.

تشمل الخدمة المقدّمة للعميل:

- منع تسرب البيانات
- مراقبة إنتاجية الموظفين و الكشف عن أنماط الخمول المتكرر
- كشف الاحتيال المؤسسي (مثل العمولات غير المشروعة أو العمل الخارجي أثناء ساعات العمل)
- و الملكية الفكرية (Know-how) حماية المعرفة
- الحد من مخاطر فقدان الكفاءات و الموظفين الرئيسيين
- التحقيق في الحوادث الأمنية

كيف يعمل النظام؟

نسخة تجريبية مجانية لمدة 30 يومًا بكامل المزايا

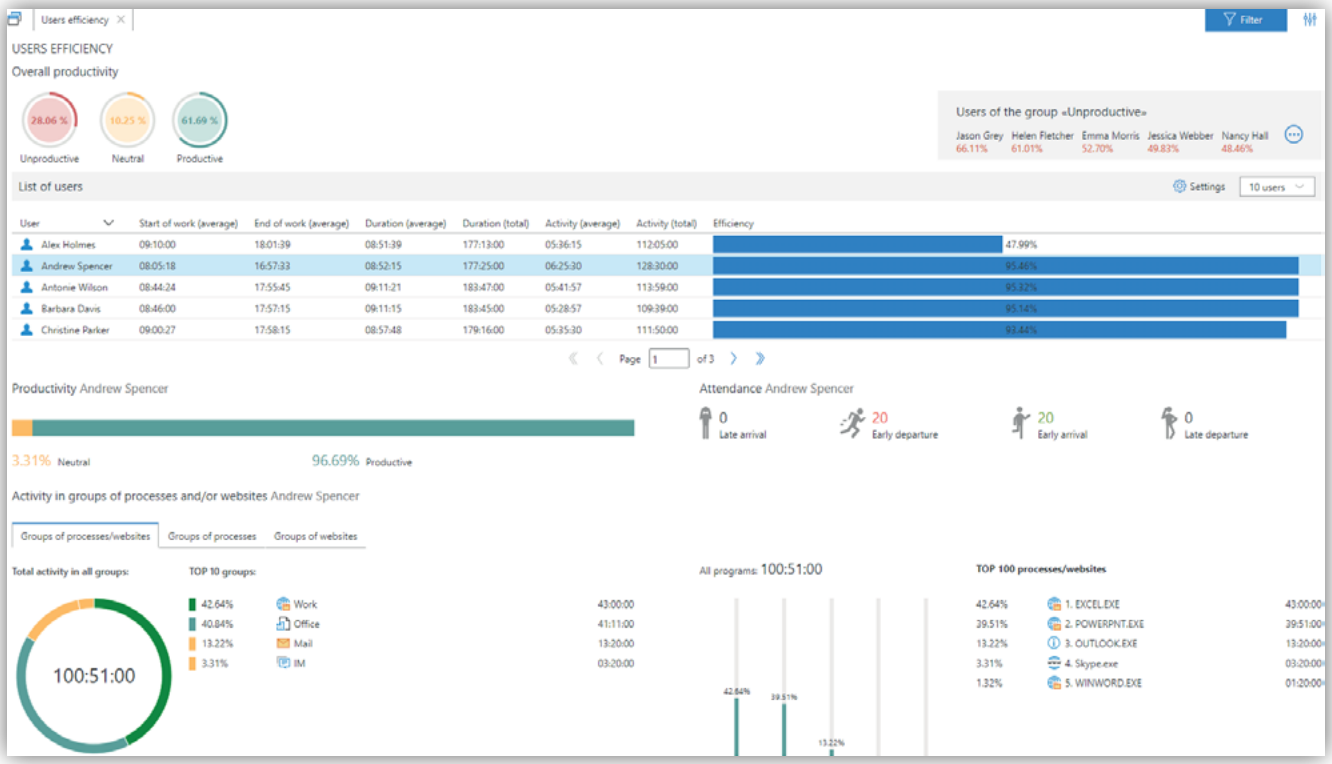
خلال الفترة التجريبية المجانية، ستقومون بإجراء تدقيق شامل لمؤسساتكم، و تحديد مشكلات حماية البيانات، و الحصول على نتائج عملية، و تلقّي نصائح خبراء حول تعزيز الأمن المؤسسي، إضافةً إلى تقييم ما إذا كانت خدمات بواسطة SearchInfrom تلبّي متطلباتكم.

المهام – الحلول

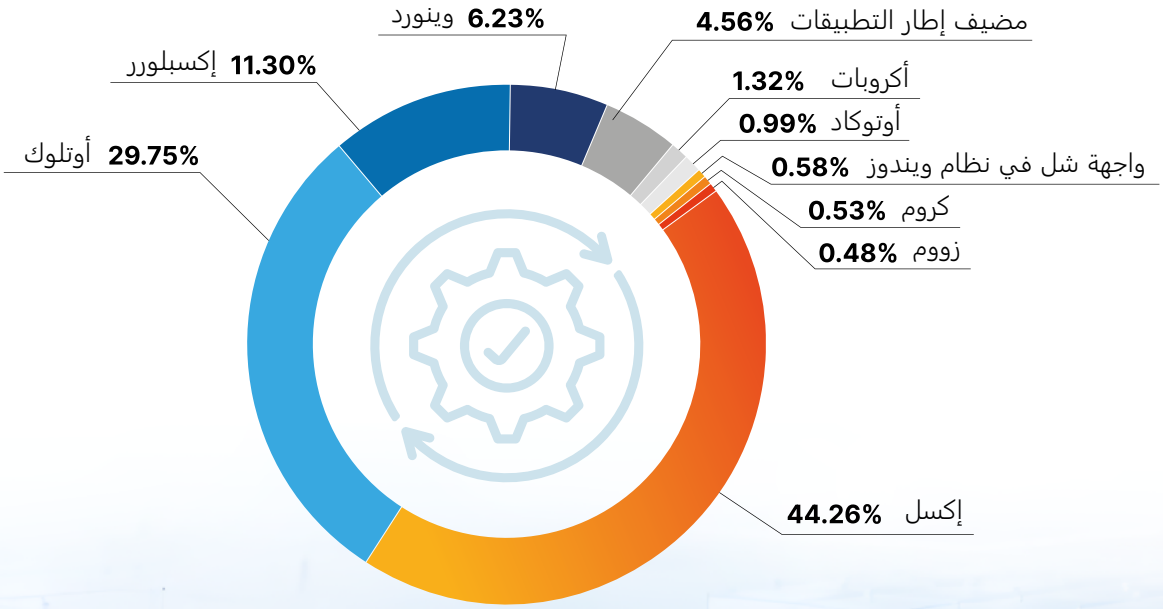
يحصل العملاء على رؤية شاملة و واضحة لأنشطة مؤسساتهم الفعلية من خلال تقارير متكاملة قائمة على البيانات.

التاريخ	الموظف المعني	التعليقات	رابط للمستندات
		الأجهزة الخارجية	
05/06/2024	جون سميث	قام موظف بتوصيل وحدة تخزين USB شخصية بجهاز كمبيوتر الشركة و حاول نسخ كمية كبيرة من البيانات. تم حظر العملية، و منع تسريب البيانات. و كشف التحقيق أن الموظف حاول نسخ قاعدة بيانات العملاء و بيعها لاحقًا لمنافس.	معلومات واقعية كاملة
		تسريبات البيانات	
21/06/2024	عمر أيدين	كشف تحليل المراسلات في تطبيق و اتساب الخاص بالشركة عن حادثة تسريب بيانات. ناقش الموظف صفقة مرتقبة مع ممثل من شركة منافسة، حيث تواصلا عبر الرسائل الفورية. و لاحقًا، شارك الموظف بعض المستندات التجارية المتعلقة بالصفقة مع المنافس عبر و اتساب.	معلومات واقعية كاملة
01/07/2024	باربرا ديفيس	كان الموظف ينوي خرق البيانات: حيث أنشأ مسودة بريد إلكتروني في صندوق بريده الشخصي على جوجل باستخدام حاسوب الشركة المحمول و أرفق بيانات مالية سرية و ملفات (بما في ذلك فاتورة هاتف). كان ذلك سيمكنه من الوصول إلى البيانات خارج نطاق الشركة بعد فترة من الوقت حتى دون إرسال البريد.	معلومات واقعية كاملة
		تزوير المستندات	
05/07/2024	دانييل ميرفي	قام موظف في قسم المشتريات بتزوير عروض تجارية واردة من الموّردين باستخدام برنامج لتحرير الصور، حيث غيّر المبالغ المذكورة في العروض.	معلومات واقعية كاملة
		التعاون مع المنافسين	
14/07/2024	بوبش غوشال	تم الكشف عن مؤشرات على تزوير مستندات. و كشف التحقيق أن الموظف كان يحرر مستندات تابعة لشركة طرف ثالث، و التي تبيّن لاحقًا أنها منافس، و كان الموظف أحد مؤسسيها المشاركين.	معلومات واقعية كاملة
20/07/2024	خالد مصطفى	تم العثور على مستندات تأسيس لشركة طرف ثالث على جهاز أحد موظفي قسم المالية. و كشف التحقيق أن مؤسّسة هذه الشركة هي زوجة الموظف. يمكن العثور على الأدلة التي تثبت أن هذه الشركة مورد دائم في قسم رابط الوثائق.	معلومات واقعية كاملة
		البحث عن عمل	
29/07/2024	جميل فريدي	تم العثور على أدلة تشير إلى أن أحد الموظفين يبحث بنشاط عن وظائف للتقديم عليها. و كان الموظف يتلقى رسائل بريد إلكتروني مرتبطة بالوظائف على: [redacted]	معلومات واقعية كاملة
		إساءة استخدام موارد الشركة	
13/08/2024	حسن دمير	أحد الموظفين يستخدم جهاز الكمبيوتر المحمول الخاص بالشركة للعب الألعاب الإلكترونية. تستخدم هذه الألعاب عبر الإنترنت أنواعًا مختلفة من ملفات تعريف الارتباط غير المرغوبة و تعرض إعلانات قد تُلحق الضرر بمعدات الشركة.	معلومات واقعية كاملة
		الموظفين المعرضين للخطر	
20/08/2024	إليف كايا	يقضي أحد موظفي قسم المبيعات بضع ساعات أسبوعيًا على مواقع المقامرة.	معلومات واقعية كاملة
23/08/2024	جين دو	كشفت مراسلات أحد الموظفين أنه يعاني من ديون كبيرة، و أن بعض الأشخاص يطالبونه بسدادها. يعمل الموظف في قسم المالية، لذلك يجب القضاء على المخاطر.	معلومات واقعية كاملة
		التخريب	
02/09/2024	كريستوفر تيرنر	حاول موظف مستقيل إلحاق الضرر بالشركة عبر حذف بعض البيانات السرية دون إمكانية استعادتها. تم إحباط محاولة الموظف بنجاح. راجع التقرير التفصيلي لمعرفة البيانات التي حاول الموظف حذفها بالضبط.	معلومات واقعية كاملة

رؤية شاملة لجميع العمليات التجارية

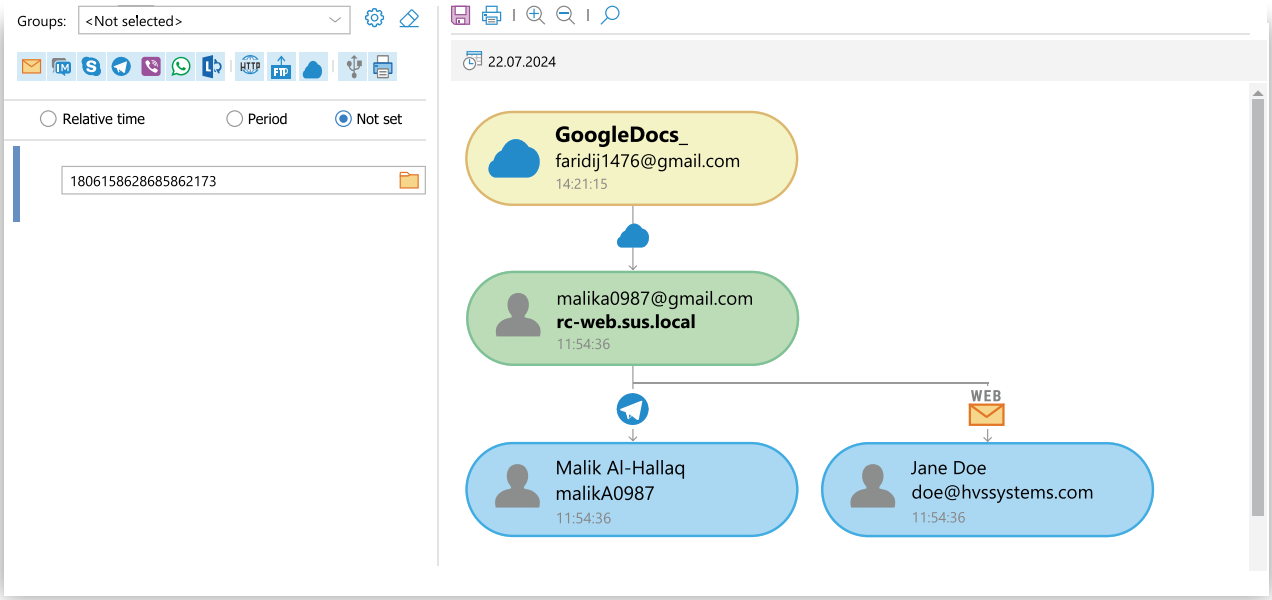


تقرير حول كفاءة المستخدمين (Report on user efficiency)



أكثر العمليات تفعيلًا (Key activated processes)

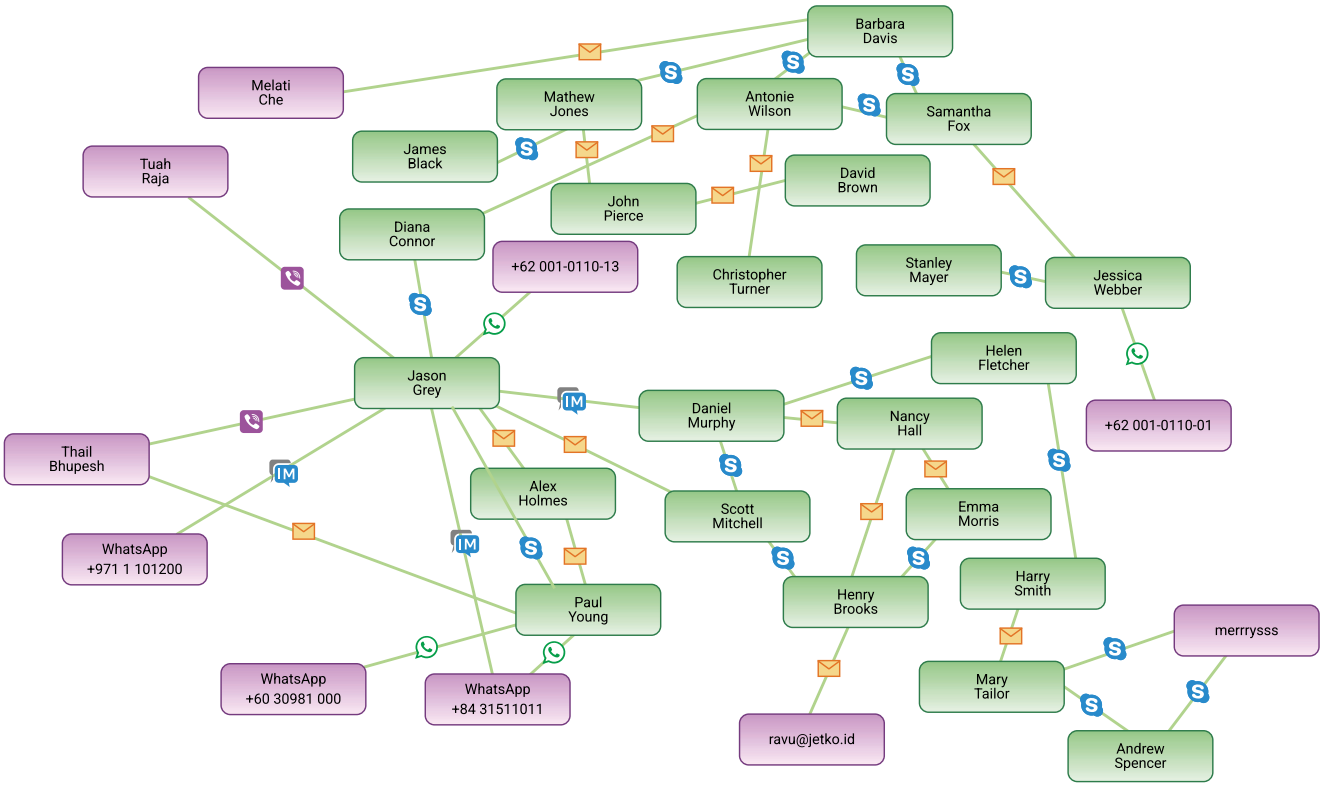
تحليلات دقيقة



مسار المحتوى (Content route)

تم تسريب تقرير مالي. و يكشف تقرير "مسار المحتوى" عن الطريق الذي سلكه المستند المُسرَّب.

يكشف تقرير الترابط جميع المستخدمين المتورطين في الحادثة الأمنية.



تقرير اتصال المستخدمين (User connection report)

المزايا

- توفير في الميزانية لن تكونوا بحاجة إلى:
  - شراء تجهيزات أو معدات
  - دفع تكاليف تراخيص البرمجيات و الدعم الفني
  - توظيف أو الاحتفاظ باختصاصيي أمن المعلومات

- نتائج دون تكاليف عمالة

  يقدّم الحل حماية متقدمة دون الحاجة إلى خبراء داخليين، متجاوزًا التحدي المتمثل في صعوبة العثور على كوادر مؤهلة في السوق.

- فعالية فورية

  يحدّد الحل الثغرات بسرعة، حيث تظهر النتائج الأولية عادةً خلال فترة التجربة المجانية التي تمتد لشهر واحد.

- احترافية حيادية

  لا يعرف محلّلونا موظفيكم معرفة شخصية، مما يساعد على القضاء على أي تحيّز أو احتمال فساد أثناء التحقيقات.

- خبرات واسعة

  يستفيد محلّلونا من قاعدة معرفية متكاملة تضم أكثر من 4,000 حالة عميل، مما يتيح لهم إعداد حلول حماية مُصمَّمة خصيصًا لتناسب صناعاتكم و تلبي متطلبات أعمالكم.

التكامل مع Microsoft 365

تتكامل حلول SearchInform بشكل كامل وسلس مع Microsoft 365

يتزايد التوجه نحو الاعتماد على الخدمات السحابية. مع انتقال التطبيقات و البيانات إلى السحابة، و إتاحة المعلومات و الوظائف عبر إصدارات قائمة على المتصفح، لم تعد وسائل الحماية التقليدية على الأجهزة الطرفية كافية.

تُعد Microsoft 365 واحدة من أكثر الخدمات السحابية شيوعًا. قد طوّرت SearchInform نظام حماية متخصّصًا لـ Microsoft 365 بهدف تأمين بياناتكم المؤسسية و حمايتها على النحو الأمثل.

- يتم تنفيذ التكامل عبر Graph API، مما يوفر للعملاء إمكانية الوصول الكامل إلى جميع و ظائف حلول الأمان المهمة.
- توفر حلول SearchInform الحماية عبر جميع خدمات Microsoft 365، بما في ذلك: Word و Excel و PowerPoint و Outlook و Teams و SharePoint و OneDrive و غيرها.

آلية العمل

من خلال تكامل سلس، يتم تحليل الملفات و المعلومات المُرسلة إلى خدمات Microsoft 365 (بما في ذلك Outlook) و حمايتها مباشرةً على الخادم بواسطة SearchInform FileAuditor و SearchInform DLP.

تشمل آليات الحماية الرئيسية لـ Microsoft 365 ما يلي:

- نموذج حماية بلا وكيل يوفّر حماية فعّالة ضمن محيط مؤسسي أصبح غير واضح الحدود.
- استخدام تحليلات قائمة على المحتوى لتحديد مضمون المستندات بدقّة عالية.
- تحليل التصنيفات المخصّصة من خلال Microsoft Information Protection.
- بيئة حماية موحّدة تغطي السحابة وبيئات Windows و macOS و Linux.
- دعم فحص الملفات في SharePoint.

تكامل FILEAUDITOR مع MICROSOFT 365

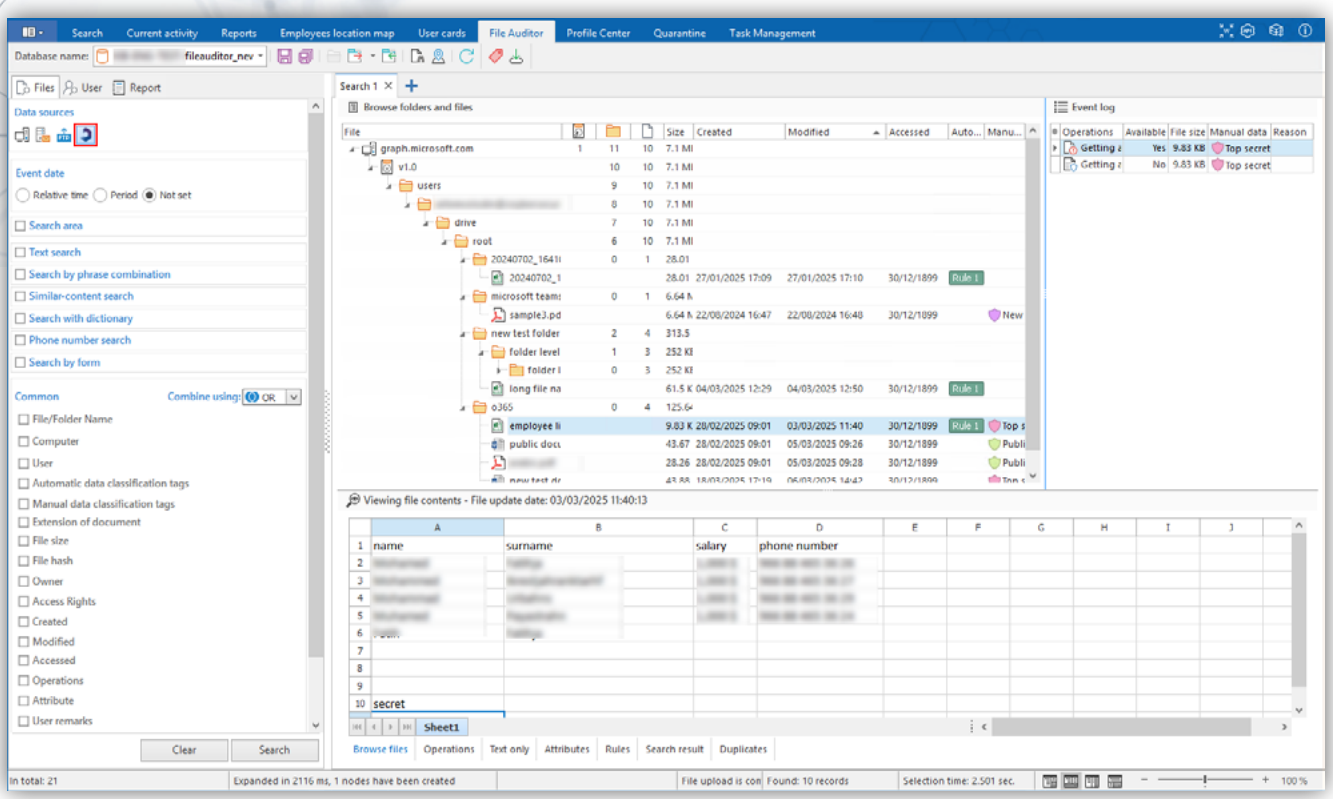
أثناء استخدام Microsoft 365، يتولى FileAuditor متابعة و رصد كافة أنشطة المستخدمين ضمن بيئة المؤسسة

يتمكّن النظام من الوصول إلى جميع مساحات العمل في Microsoft 365 التي يتفاعل معها المستخدمون.

يقوم الحل بفحص هذه المساحات و تصنيف الملفات المخزنة فيها باستخدام تحليلات قائمة على المحتوى.

في الوقت نفسه، يقوم FileAuditor بتنظيم الملفات تلقائيًا في فئات مخصّصة. فعلى سبيل المثال، عند ظهور ملف في محادثة عبر Teams، ينشئ الحل قسمًا مخصّصًا تحت اسم "ملفات محادثات Microsoft Teams" لتخزينه. تساعد هذه الأتمتة في تقليل الأعباء الروتينية على محللي أمن المعلومات و تعزّز كفاءة الأمان بشكل عام.

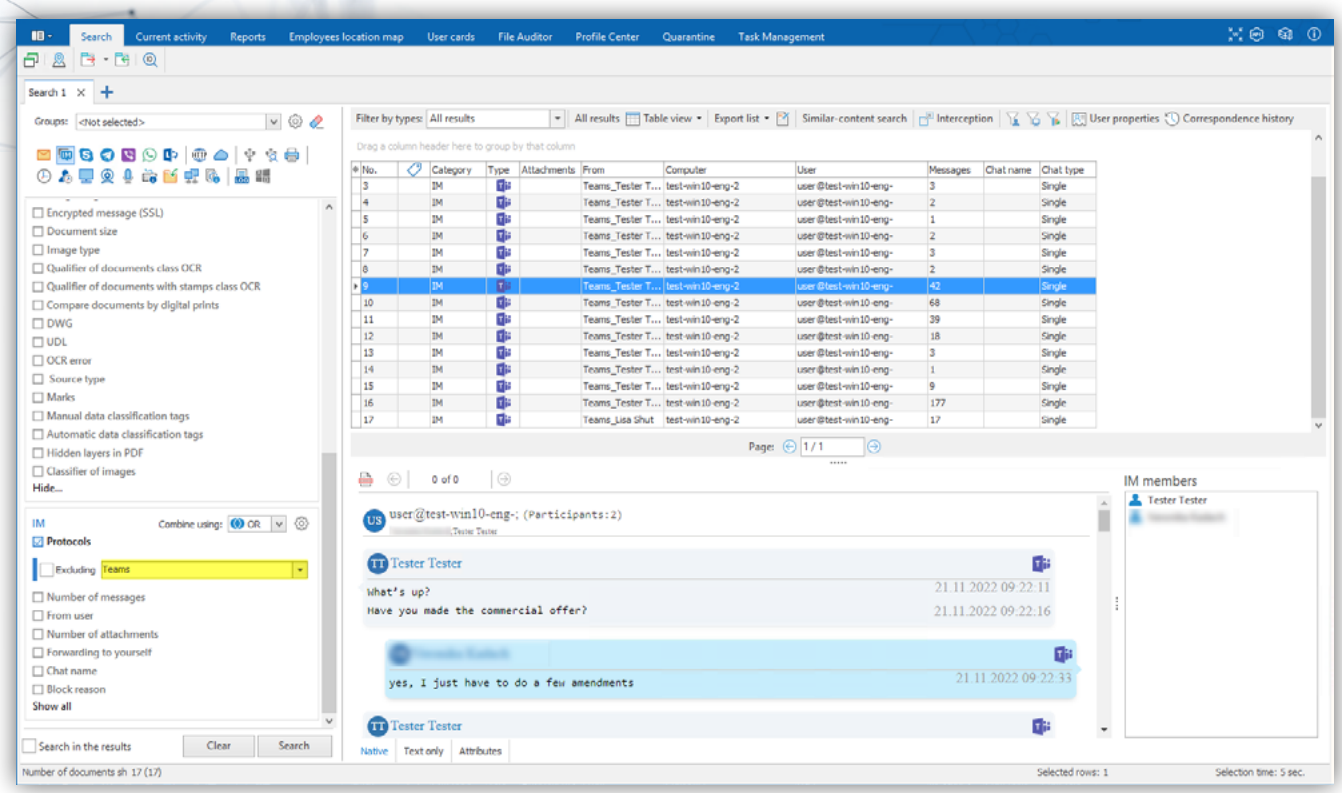
يقوم FileAuditor بتحليل جميع الملفات و إسناد تسميات سرية لها استنادًا إلى محتوى المستند، و نوع المعلومات، و مستوى حساسيتها. يتيح ذلك تقييمًا دقيقًا لمدى أهميتها و تطبيق السياسات الأمنية المناسبة.



نتائج فحص FileAuditor باستخدام Microsoft 365

تكامل DLP مع MICROSOFT 365

يوفّر تكامل SearchInform DLP مع Microsoft 365 للمستخدمين وصولًا كاملًا إلى جميع وظائف DLP القياسية.



1 يقوم الحل بالتحكم في نقل البيانات عبر جميع خدمات Microsoft 365.

2 يعتمد المبدأ التشغيلي على تحليل سياق و محتوى الملف لتحديد نوعه، و مستوى سريته، وما إذا كان خاضعًا لسياسات أمنية محددة. يسهم التكامل مع FileAuditor في تعزيز دقة التحليل و تقليل تكاليف تشغيل نظام DLP.

3 تظل جميع إمكانات التحليلات المتقدمة التقليدية و الأدلة الجنائية الإلكترونية متاحة. يتلقى محلل أمن المعلومات تفاصيل شاملة عن الحادث، بما في ذلك الرسالة الأصلية، و الملفات المنقولة (بصيغتها الأصلية)، و معلومات المرسل و المستلم.

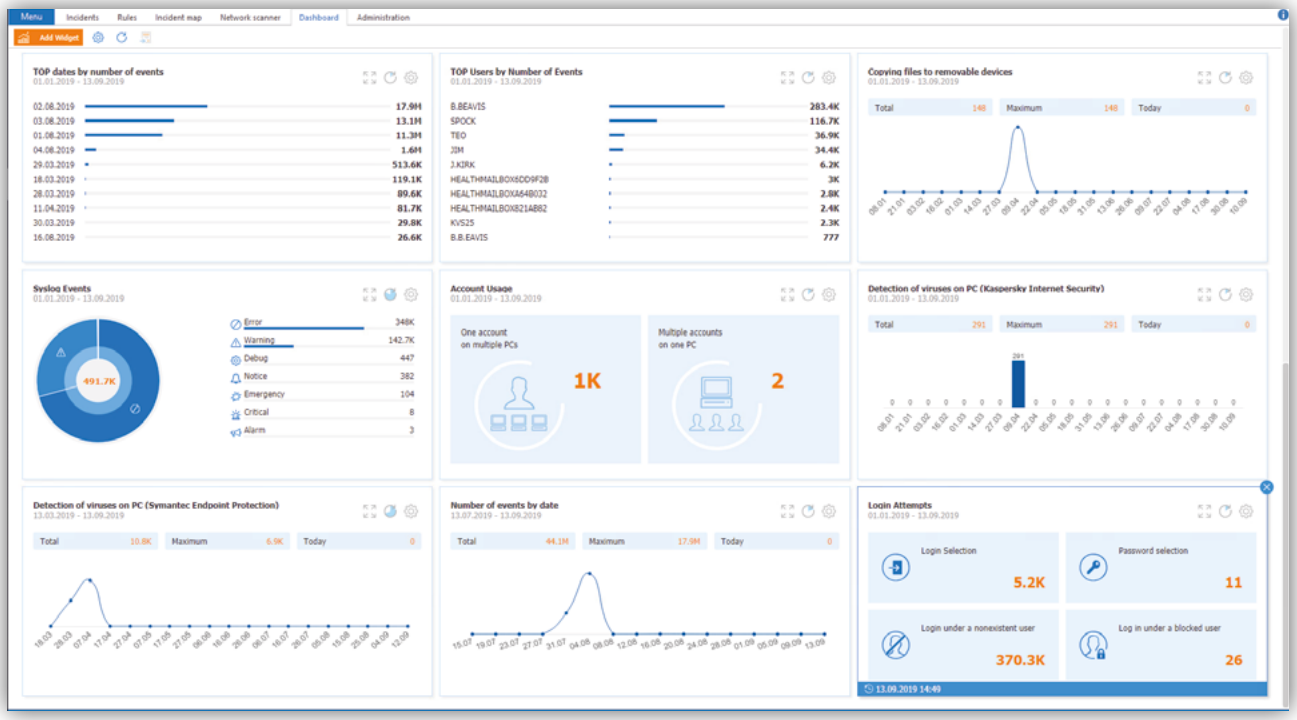
SearchInform SIEM

تتكوّن البنى التحتية الحديثة لتقنية المعلومات في المؤسسات من عدة أنظمة حيوية، مثل جدران الحماية، و أنظمة التشغيل، و خوادم البريد الإلكتروني، و قواعد البيانات، و أجهزة الشبكة.
و تُعد هذه الأنظمة أهدافًا رئيسية للجهات الخبيثة، مما يستلزم اتخاذ تدابير أمنية متخصصة.

- منصة SIEM جاهزة للاستخدام مباشرة
- قواعد الترابط يتم إنشاؤها بنقرتين فقط

المراقبة التلقائية لأحداث الأمان

SearchInform SIEM هو حل شامل لجمع و تحليل أحداث الأمان و الاستجابة للحوادث الأمنية في الزمن الحقيقي. يقوم النظام بتجميع البيانات من مصادر متعددة، و يُجري تحليلات متقدمة، و يسجّل الحوادث تلقائيًا، و يُرسل التنبيهات إلى المسؤولين المكلّفين.



لوحة إحصاءات الأحداث (Event statistics dashboard)

SearchInform SIEM يكشف:

- الأوبئة الفيروسية و الإصابات المنفصلة
- محاولات للوصول غير المصرح به إلى البيانات
- تخمين كلمات المرور للحسابات
- الحسابات النشطة للموظفين المفصولين و التي تم نسيان حذفها
- أخطاء تكوين المعدات
- إساءة استخدام درجة حرارة التشغيل المسموح بها
- إزالة البيانات من الموارد الهامة
- إساءة استخدام موارد الشركة
- إزالة الأجهزة الافتراضية و اللقطات
- ربط معدات جديدة بالبنية التحتية لتكنولوجيا المعلومات
- تعديل سياسات المجموعة
- استخدام برنامج TeamViewer، الوصول عن بعد إلى موارد الشركة
- الأحداث الحرجة في وسائل الحماية
- الأخطاء الأخرى و الفشل في نظم المعلومات

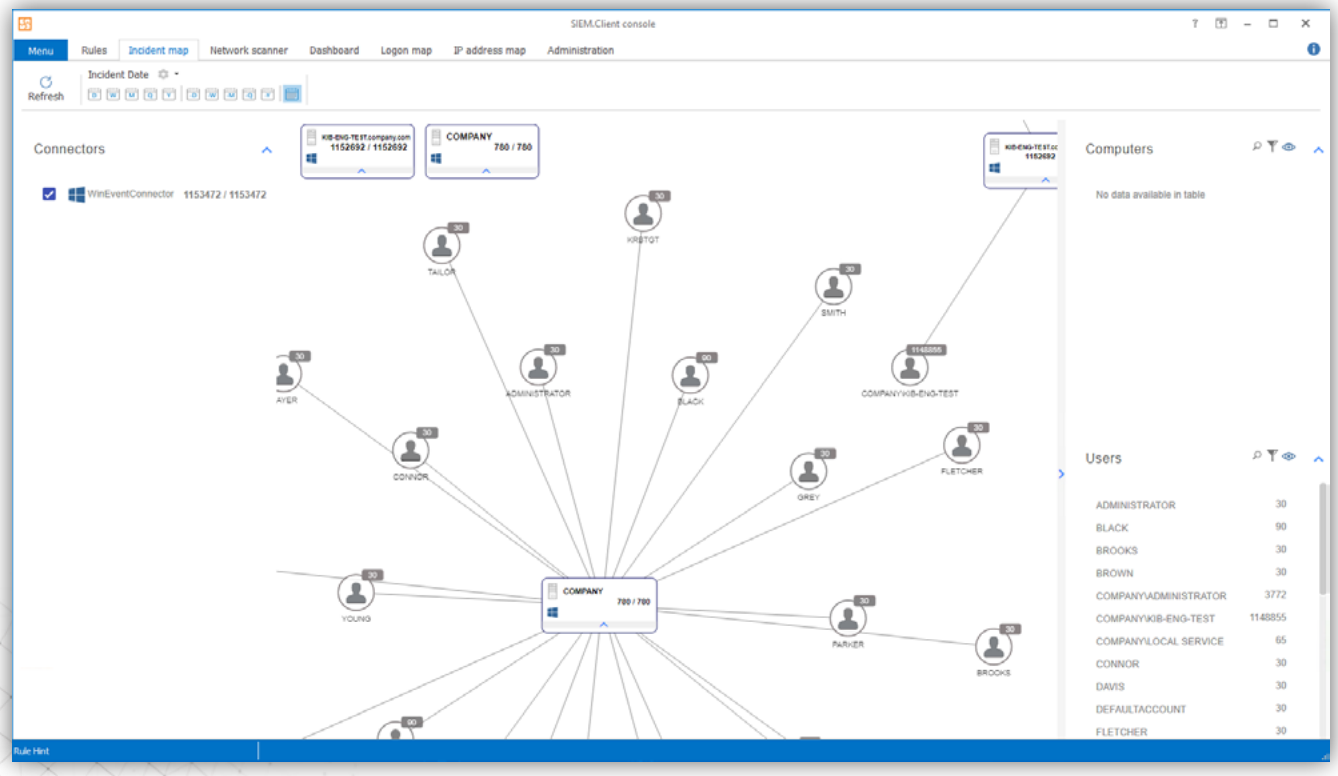
قواعد الارتباط الجاهزة في SEARCHINFORM

عند التثبيت، يزوّد النظام فرق أمن المعلومات بأكثر من 350 سياسة أمان جاهزة للاستخدام، مع إمكانات كاملة لتخصيص القواعد القائمة، و أدوات مرنة لإنشاء السياسات (بما في ذلك خاصية ربط المستخدمين). و يمكن لفرق الأمن تعديل القواعد المُعرّفة مسبقًا، و إنشاء سياسات مخصّصة، و الجمع بين السياسات الجاهزة و تلك التي يحددها المستخدم.

تستند القواعد المُعرّفة مسبقًا إلى هذه المكوّنات الأساسية للبنية التحتية:

- أنظمة التشغيل
- خوادم البريد الإلكتروني
- متحكمات النطاق ومحطات العمل
- خوادم ومحطات عمل Linux
- أنظمة إدارة قواعد البيانات (DBMS)
- أنظمة منع فقدان البيانات (DLP)
- خوادم الملفات
- بيئات الافتراضية
- برامج مكافحة الفيروسات (Antiviruses)
- الجدران النارية و أجهزة أمن الشبكات
- جميع الأجهزة المتوافقة مع بروتوكول Syslog

يمكن تهيئة قواعد الارتباط المتقاطع لاكتشاف الحوادث الأمنية المعقّدة من خلال تحليل الأحداث المترابطة عبر مصادر بيانات متعددة.



شاشة عرض حوادث أمن المعلومات (Incident display screen)

قواعد الارتباط الجاهزة في SearchInform SIEM

سيرفرات البريد:

- الوصول غير المرغوب فيه إلى صندوق البريد
- تغيير ملكية صندوق البريد
- منح الوصول إلى صندوق البريد

بيئة المحاكاة الافتراضية:

- أحداث تسجيل الدخول/الخروج لـ VWview/VMware
- كلمات مرور غير صحيحة
- حذف اللقطات

من أجل التحكم في نطاق الشبكة (دومين) و محطات العمل

- تمكين / إضافة حساب مؤقت
- حساب واحد على أجهزة كمبيوتر متعددة
- تخمين كلمة المرور و كلمات المرور القديمة

التحكم في الوصول إلى الموارد

- منع الوصول غير المصرّح به إلى الملفات الحرجة
- تعيين مؤقت لأذونات الملفات و المجلدات
- أنماط غير طبيعية للوصول المتعدد المستخدمين إلى الملفات

كيف يعمل النظام؟

1 يجمع الأحداث من مصادر مختلفة للبرامج و الأجهزة: معدات الشبكة، و برامج الطرف الثالث، و أدوات الأمان، و نظام التشغيل.

2 يحلل الأحداث و يولّد الحوادث وفقًا للقواعد و يكشف التهديدات عن طريق تحديد العلاقات الارتباطية، بما في ذلك الارتباطات المتبادلة للأحداث و/ أو الحوادث.

3 يقوم تلقائيًا بإعلام الموظفين المسؤولين عند و قوع الحوادث.

4 يطبع و يفصل الحوادث لمزيد من التحقيق؛ يحدد نوع و مصدر الحادث، عند التكامل مع AD – من المحتمل أن يشارك المستخدم في الحدث.

المزايا

- تنفيذ سريع دون الحاجة إلى تكوين مسبق طويل (يمكن تشغيل البرنامج في يوم واحد فقط)، النتائج فورية.
- سهل الاستخدام: يمكن التعامل مع البرنامج من قبل موظف ليس لديه مهارات معينة في تكنولوجيا المعلومات أو معرفة بلغات البرمجة – لا يلزم أي منها لإنشاء قواعد الارتباط و الارتباط المتبادل.
- متطلبات أجهزة منخفضة، الترخيص الواضح، تكلفة ملكية مريحة.
- التحليلات "خارج الصندوق": يأتي النظام مع مجموعة من القواعد الجاهزة و بأخذ في الاعتبار خبرات و مهام الشركات من جميع مجالات الأعمال و قطاعات الاقتصاد.
- إدارة الحوادث: من الممكن إنشاء تحقيق بناءً على حادث واحد أو أكثر.

التكامل السلس مع نظام Risk Monitor يعزز أمن معلومات الشركة و يجعل من الممكن إجراء تحقيق شامل في الحادث و جمع الأدلة المطلوبة.

جهات الاتصال

أمريكا اللاتينية

البريد الإلكتروني: s.bertoni@searchinform.com

شمال أفريقيا

البريد الإلكتروني: m.sayari@searchinform.com

جنوب شرق آسيا

البريد الإلكتروني: order@searchinform.com

روسيا

البريد الإلكتروني: info@searchinform.ru

كازاخستان

البريد الإلكتروني: e.matushenok@searchinform.ru

الشرق الأوسط وشمال أفريقيا

البريد الإلكتروني: uae@searchinform.com

تركيا

البريد الإلكتروني: salesturkiye@searchinform.com

يمكنكم تجربته و الحصول
على موارد مفيدة على

searchinform.com

عملائنا