safetica

Podręcznik użytkownika

PRZEWODNIK PO MODULE AUDYTOR

SAFETICA OCHRONA PRZED WYCIEKIEM DANYCH

Zapraszam Cię do bezpłatnego testu, dzięki któremu dowiesz się czy kluczowe dla Twojej firmy dane są bezpieczne, czy też grozi im wyciek.

Niniejszy przewodnik przeprowadzi Cię przez proces audytu Safetica, dzięki któremu dowiesz się, w jaki sposób pracują Twoi pracownicy, czy i z jakich nośników zewnętrznych korzystają oraz jakie strony WWW odwiedzają.
Dokument pomoże Ci również w interpretacji uzyskanych wyników.

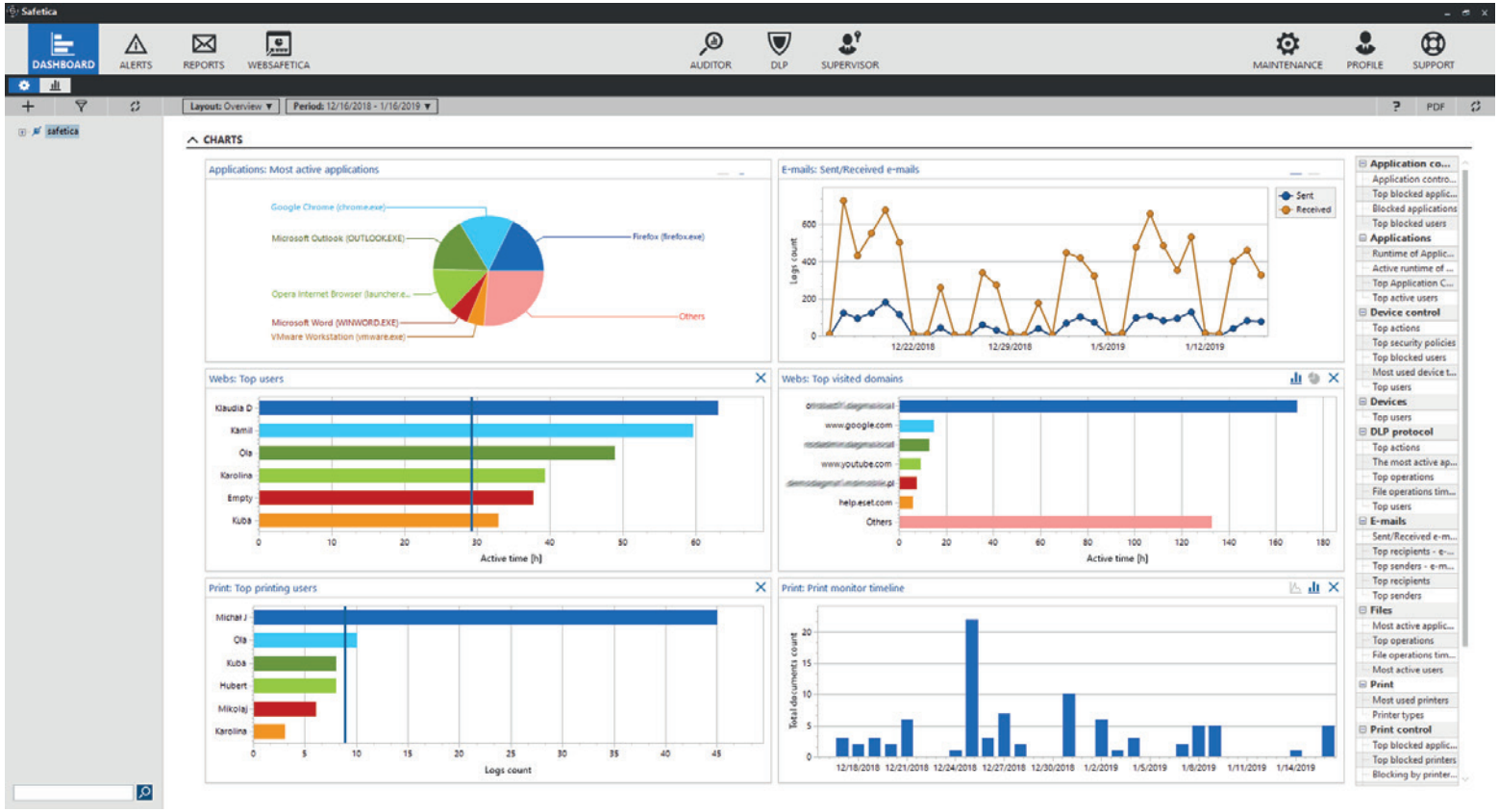
Liczę, że wspomniany test pozwoli Ci uzyskać kluczową dla Ciebie informację nt. bezpieczeństwa danych w Twojej firmie. Liczę również, że dowiedzie, że intuicyjność obsługi rozwiązania Safetica i jego skuteczność spełni Twoje oczekiwania.
W razie pytań pozostaję do Twojej dyspozycji.

Mateusz Piątek
Product Manager Safetica
tel. 32 259 11 67 / 532 570 255
piatek.m@dagma.pl

ZADANIE 1

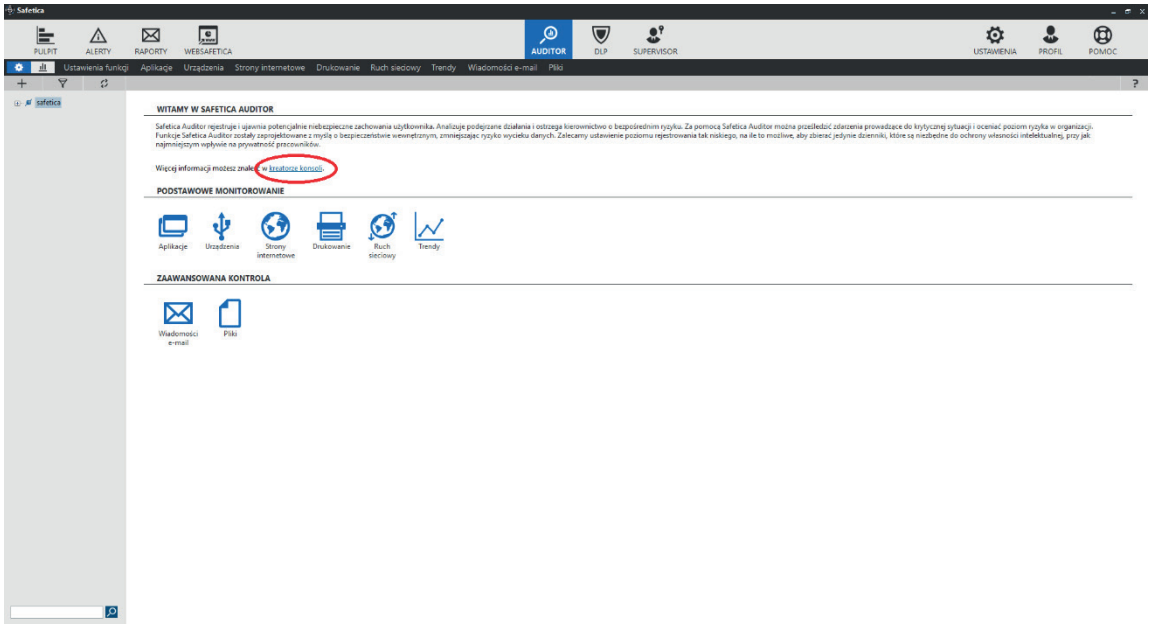
Ustawienia początkowe

Zacznijmy od podstaw. Zakładam, że jesteś już po instalacji konsoli, serwera Safetica, bazy danych i klientów na stacjach końcowych. Jeśli nie, skorzystaj proszę z **przewodnika instalacji**, a następnie wróć do niniejszego dokumentu. Po uruchomieniu konsoli zarządzającej Safetica powinieneś zobaczyć poniższy widok:



Zacznij od zmiany języka programu, na język polski (jeśli Twoja konsola działa w języku polskim, możesz pominąć ten krok). W tym celu kliknij w prawym górnym rogu w sekcję ***Profile***, a następnie ***Language***. Wybierz polski i potwierdź w prawym górnym rogu za pomocą przycisku ✓

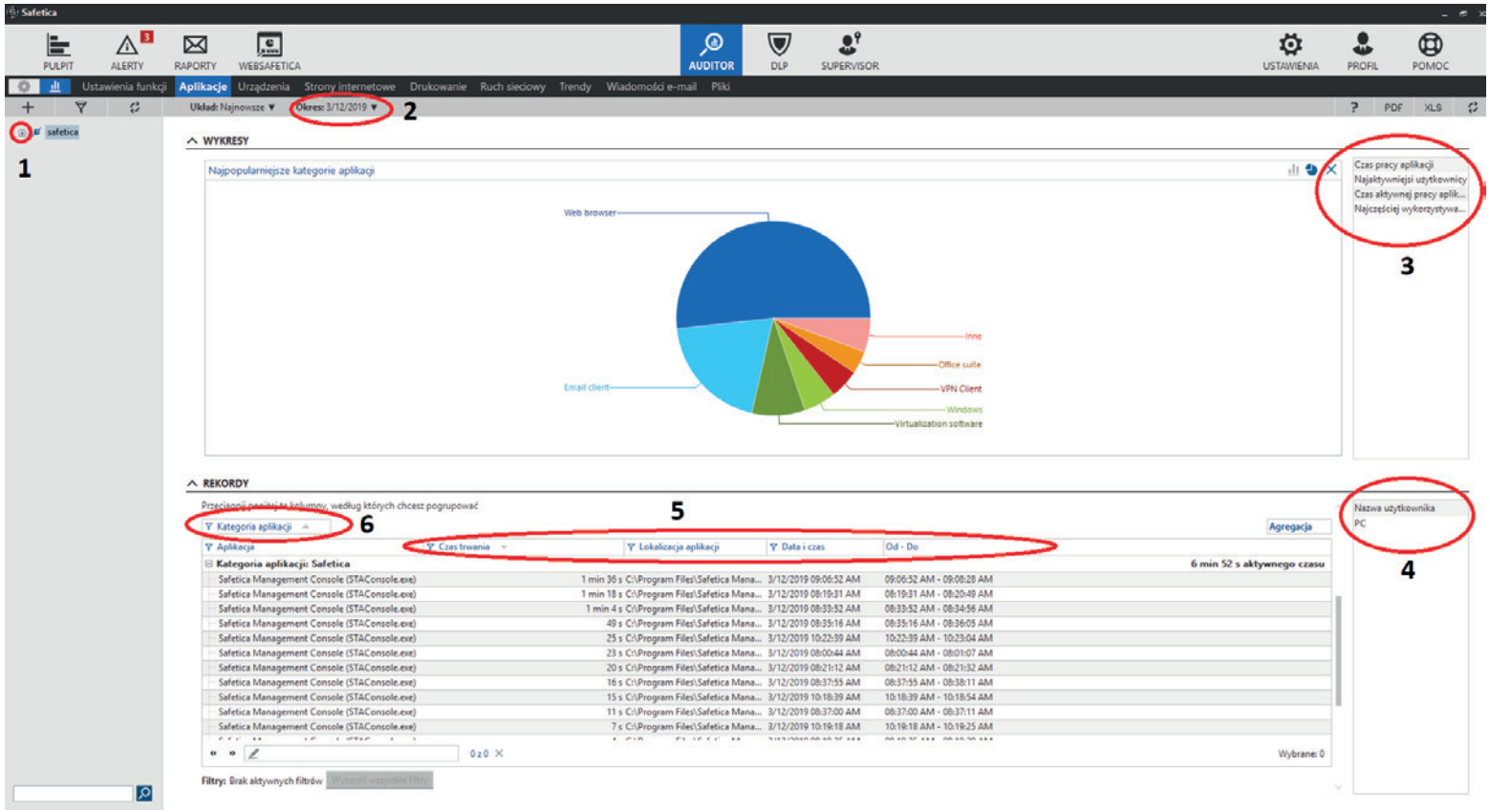
Kliknij teraz w sekcję ***Audytor*** i zapoznaj się z ***Kreatorem konsoli***, klikając w hiperłącze jak na obrazku poniżej:



Po zapoznaniu się z zawartością ***Kreatora konsoli*** przejdź - do zakładki ***Ustawienia Funkcji*** i upewnij się, że każdy element został włączony. Taka konfiguracja Audytora pozwoli zbierać informacje nt. tego, co dzieje się na każdym podłączonym do Safetica komputerze (listę komputerów zobaczysz w tzw. drzewku, widocznym po lewej stronie ekranu – jeśli nie widzisz komputerów sprawdź „**WDROŻENIE SAFETICA AGENT I SAFETICA CLIENT**” w **Instrukcji obsługi**).

Audytor zgromadzi dane o:

- aplikacjach uruchamianych przez użytkowników,
- podłączanych urządzeniach,
- odwiedzanych stronach internetowych,
- drukowanych dokumentach,
- ruchu sieciowym,
- wiadomościach e-mail,
- plikach.



1. **„Drzewo" podłączonych komputerów i użytkowników, których pracę monitoruje Safetica.** Możesz rozwinąć wspomniane drzewo, aby analizować dane np. tylko dla jednej osoby/komputera. W przypadku zaznaczenia - jak na zrzucie (całej grupy) - widok w części głównej (wykresy i rekordy) będą dotyczyły całej monitorowanej organizacji.
2. W tym miejscu możesz wybrać **czas analizowanych danych**. Jeśli chcesz zobaczyć, co działo się *„dziś"* – wybierasz tę opcję.
3. **Wykresy „Drag & Drop"** – każdy z określonych typów danych możesz przesunąć do głównego okna, by wyświetlić je w formie wykresu.
4. **Filtr „drag & drop"** – każdy z parametrów w tej kolumnie możesz przeciągnąć na pasek filtrów (pkt. 5) lub do nagłówka (pkt. 6) aby dostosować ilość oraz szczegółowość wyświetlanych informacji.
5. **Pasek filtrów** – możesz dostosować ilość oraz szczegółowość wyświetlanych informacji, dobierając parametry z kolumny po prawej stronie (pkt. 4).
6. **Filtr w nagłówku** – podstawowy parametr wykorzystywany do filtrowania wyświetlanych wyników; wybierany z kolumny (pkt. 4) lub paska (pkt. 5).

Zapoznałeś się już wstępnie z podstawowym poruszaniem się po menu – przejdźmy zatem do analizy poszczególnych aspektów.

ZADANIE 2

Analiza aplikacji

Aby dobrze zinterpretować potencjalne zagrożenia, musisz znać działania podejmowane przez użytkowników firmowych komputerów. Zobaczmy zatem, jakie aplikacje uruchamiali i ile czasu spędzili w nich Twoi pracownicy w ostatnim czasie. Warto zauważyć, że Safetica mierzy aktywny czas aplikacji – a więc czas, który użytkownik realnie spędził w danej aplikacji.

Na podstawie zakładki aplikacji możemy zdobyć wiedzę:

- czy pracownicy korzystają z aplikacji stanowiących potencjalne zagrożenie dla bezpieczeństwa sieci firmowej?
- czy pracownicy uruchamiają aplikacje niepowiązane bezpośrednio z ich pracą?
- czy pracownicy uruchamiają aplikacje, na które firma nie ma licencji?
- czy ilość zakupionych licencji danego programu pokrywa się z liczbą osób z niego korzystających?
- ile czasu pracownicy spędzają w poszczególnych aplikacjach?

Aby sprawdzić, jakie aplikacje uruchamiali pracownicy - przejdź do zakładki ***aplikacje***, a następnie wybierz:

1. Zakres danych -> zaznacz „*dziś*"
2. Użytkownicy -> zaznacz „*cała organizacja*"
3. Wyciągnij do nagłówka filtr „*kategoria aplikacji*"
4. Pasek filtrów skonfiguruj w taki sposób, aby wyświetlał następujące informacje:
   a. *Nazwa użytkownika*
   b. *Aplikacja*
   c. *Lokalizacja aplikacji*
   d. *Data i czas*
   e. *Czas trwania*
   f. *Od-Do*

Następnie zapoznaj się z zawartością rekordów, zwracając szczególną uwagę na poniższe aspekty:

- czy pracownicy uruchamiają aplikacje w kategoriach, które stanowią potencjalny wyciek danych, takich jak FTP Clients czy File synchronization?
- czy aplikacje w kategorii „*unknown*" są Ci znane?

ZADANIE 3

Analiza urządzeń

Jednym z potencjalnych miejsc wycieku danych są urządzenia podłączane do firmowych komputerów. Zobacz, jakie urządzenia instalowali Twoi pracownicy i zwróć uwagę:

- czy pracownicy podłączają urządzenia, których nie powinni używać w firmie?
- jak często takie sytuacje mają miejsce?

Przejdź do zakładki ***urządzenia***, a następnie wybierz:

1. Zakres danych -> zaznacz *„dziś"*
2. Użytkownicy -> zaznacz *„cała organizacja"*
3. Do nagłówka filtru dodaj *„typ urządzenia"* oraz niżej *„czynność"*
4. Pasek filtrów skonfiguruj w taki sposób, aby zawierał następujące informacje:
   a. *Nazwa użytkownika*
   b. *Opis*
   c. *Dostawca*
   d. *Identyfikacja*
   e. *Typ interfejsu*
   f. *Data i czas*

Przy takiej konfiguracji zyskujesz podgląd wszystkich podłączanych do komputerów urządzeń. Po rozwinięciu wszystkich opcji, możesz kliknąć w *„szczegóły"* by otrzymać więcej informacji na temat podłączanego urządzenia.

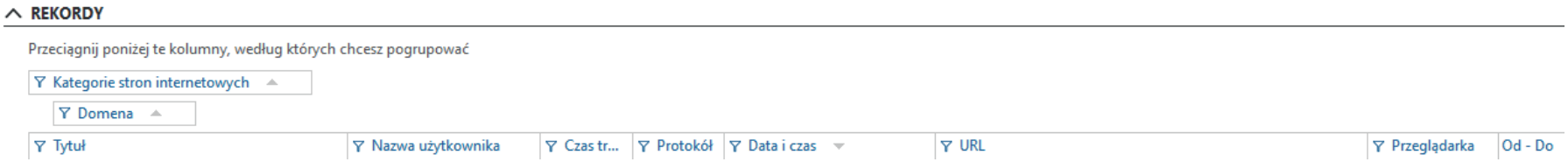
ZADANIE 4

Strony internetowe

Wiesz już, jakie urządzenia podłączają Twoi pracownicy oraz z jakich aplikacji korzystają. Nie wiesz jednak, co dokładnie robią w poszczególnych aplikacjach, np. w przeglądarkach internetowych. Czy wchodzą na strony narażające firmę na ryzyko wycieku danych, takie jak chmury, serwisy umożliwiające wymiany plików, czy prywatne skrzynki mailowe? Czy pracownicy w godzinach pracy realizują czynności inne niż służbowe?

Możesz łatwo to zweryfikować przechodząc do zakładki ***strony internetowe***:

1. Zakres danych -> zaznacz „*dziś*"
2. Użytkownicy -> zaznacz „*cała organizacja*"
3. Do nagłówka filtru dodaj „*Kategorie stron internetowych*" oraz „*Domena*"
4. Pasek filtrów skonfiguruj w taki sposób, aby zawierał następujące informacje:
   a. *Tytuł*
   b. *Nazwa użytkownika*
   c. *Czas trwania*
   d. *Protokół*
   e. *URL*
   f. *Przeglądarka*
   g. *Data i czas*



Przy tak ustawionych filtrach zobaczysz co robili Twoi pracownicy na służbowych komputerach. Informacje, jakie możesz uzyskać korzystając z tej zakładki, to odpowiedzi między innymi na pytania:

- czy pracownicy korzystają ze stron internetowych mogących stanowić zagrożenie dla bezpieczeństwa firmowych danych?
- ile czasu pracownicy realnie spędzają na czynnościach niezwiązanych z pracą?
- czy pracownicy wchodzą na strony internetowe, które nie są zabezpieczone szyfrowanym połączeniem (https)?
- czy pracownicy korzystają wyłącznie z sugerowanych przeglądarek internetowych?

ZADANIE 5

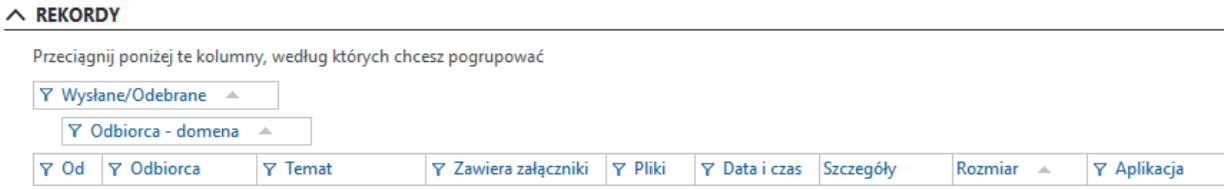
Wiadomości e-mail

Kolejnym potencjalnym źródłem wycieku danych może być poczta elektroniczna. Pomimo często stosowanych polityk bezpieczeństwa, zabraniających przesyłania kluczowych danych za pośrednictwem maila poza firmową domenę, pracownicy potrafią ominąć ustanowione reguły.

Z pomocą audytora możesz przeanalizować wiadomości e-mail jakie wysyłają Twoi pracownicy. Safetica została skonstruowana w taki sposób, aby administrator miał wiedzę o potencjalnym wycieku danych, a jednocześnie organizacja nie była narażona na ewentualne zarzuty dotyczące naruszania prywatności pracowników.

Aby sprawdzić, czy poczta e-mail stanowi ryzyko dla bezpieczeństwa danych w Twojej firmie wybierz zakładkę ***e-mail***, a następnie:

1. Zakres danych -> zaznacz „*dziś*"
2. Użytkownicy -> zaznacz „*cała organizacja*"
3. Do nagłówka filtru dodaj „*Wysłane/Odebrane*" oraz „*Odbiorca - domena*"
4. Pasek filtrów skonfiguruj w taki sposób, aby zawierał następujące informacje:
   a. *Od*
   b. *Odbiorca*
   c. *Temat*
   d. *Zawiera załączniki*
   e. *Pliki*
   f. *Data i czas*
   g. *Szczegóły*
   h. *Rozmiar*
   i. *Aplikacje*



Przy tak ustawionych filtrach zobaczysz jakie e-maile zostały odebrane i wysłane przez Twoich pracowników. Zapoznaj się z wynikami, zwracając szczególną uwagę na to:

- czy pracownicy wysyłają e-maile i załączniki poza domenę firmową?

ZADANIE 6

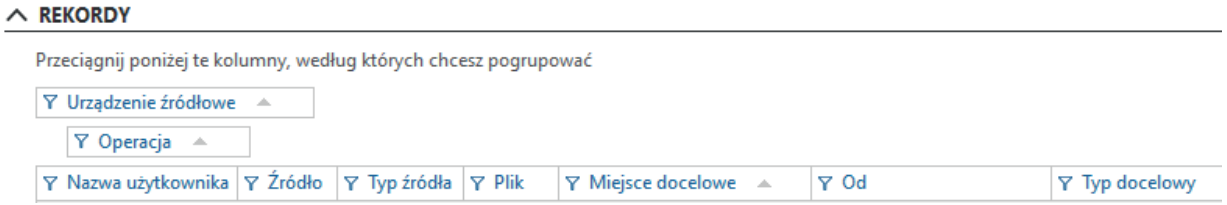
Pliki

Ostatnim elementem, na który warto zwrócić uwagę, jest historia działań pracowników na plikach. Funkcja ta może być szczególnie przydatna w sytuacji, w której np.:

- chcemy odnaleźć zagubiony plik;
- wiemy, że plik został wysłany np. e-mailem i chcemy sprawdzić historię jego powstania;
- chcemy wiedzieć kto i jakie operacje wykonywał na danym pliku.

Aby zapoznać się z wspomnianymi danymi przejdź do zakładki ***pliki***, a następnie wybierz:

1. Zakres danych -> zaznacz *„dziś"*
2. Użytkownicy -> zaznacz *„cała organizacja"*
3. Do nagłówka filtru dodaj *„Urządzenia źródłowe"* oraz *„Operacja"*
4. Pasek filtrów skonfiguruj w taki sposób, aby zawierał następujące informacje:
   a. *Nazwa użytkownika*
   b. *Źródło*
   c. *Typ źródła*
   d. *Plik*
   e. *Miejsce docelowe*
   f. *Od*
   g. *Typ docelowy*



Przy takim ustawieniu filtrów, zobaczysz jakie operacje były wykonywane na wszystkich plikach użytkowników – dzięki temu masz możliwość identyfikacji wycieków danych. W zakładce ***pliki*** znajdziesz odpowiedzi między innymi na pytania, czy pracownicy kopiują dane na dyski chmurowe, czy pracują na zasobach sieciowych oraz czy pobierają pliki z Internetu? Odpowiedzi na te pytania mogą wskazać na potencjalne luki w systemie.

ZADANIE 7

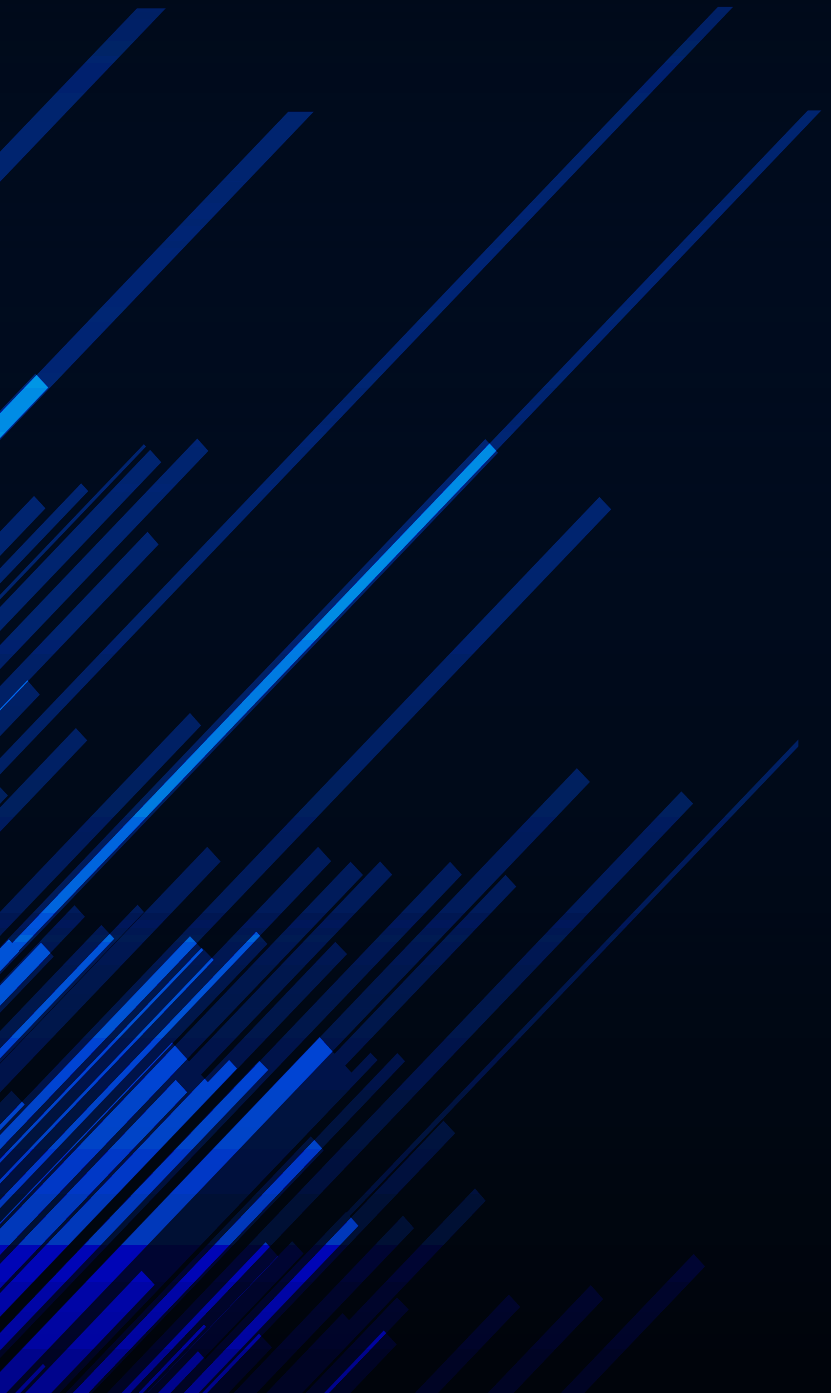
Raportowanie

Zapoznałeś się z zawartością poszczególnych zakładek, dzięki temu możesz analizować poziom bezpieczeństwa danych w swojej firmie. Pomoże Ci w tym przejrzysty raport, który możesz w dowolnym momencie wygenerować. Dzięki temu będziesz wiedzieć, jak działają pracownicy i jak zmienia się ich zachowanie w czasie.

Aby wygenerować raport, przejdź do sekcji ***WebSafetica*** (w lewym górnym rogu konsoli zarządzającej), a następnie zaloguj się tak jak do konsoli zarządzającej. Uwaga – jeśli strona nie wczytuje się prawidłowo upewnij się, że podczas procesu instalacji zainstalowałeś moduł *WebSafetica*.

Po uruchomieniu ***WebSafetica*** po lewej stronie wybierz panel kontrolny, a następnie klikając w przycisk  znajdujący się po prawej stronie wygeneruj ***Audyt bezpieczeństwa*** swojej organizacji. Postaraj się przeanalizować poszczególne aspekty bezpieczeństwa swojej organizacji.

Moduł audytora, który testowałeś, powinien wskazać Ci obszary, które mogą stanowić potencjalne ryzyko dla bezpieczeństwa danych w Twojej organizacji. Audyt, który wygenerowałeś powinien wykazać przepływ danych w organizacji oraz wskazać, czy pracownicy nie dopuszczają się do incydentów bezpieczeństwa. Jeśli chciałbyś dowiedzieć się, jak zabezpieczyć swoją organizację przed wyciekiem danych lub zyskać wiedzę na temat tego co dzieje się z kluczowymi dla Twojej firmy informacjami, skontaktuj się ze swoim opiekunem handlowym, mającym w ofercie rozwiązanie Safetica.



safetica

Dystrybucja w Polsce:

DAGMA

Bezpieczeństwo IT

ul. Bażantów 4/2, 40-668 Katowice

tel. 32 793 11 00 / handel@dagma.pl

www.safetica.pl