Logsign

SECURIVY

Zadbaj o cyberbezpieczeństwo. Zmniejsz ryzyko ataku. Zapanuj nad chaosem.

Platforma do zarządzania procesami cyberbezpieczeństwa w firmie

Prosta. Szybka. Jednolita. Skalowalna.

Logsign pomaga organizacjom poprawić cyberbezpieczeństwo, zapobiec zagrożeniom, zapanować nad chaosem w firmowej infrastrukturze IT, a także zapewnić zgodność z normami i przepisami. Narzędzie odpowiada za gromadzenie i przechowywanie danych, na co dzień generowanych w systemach informatycznych organizacji, a także ich indeksację w celu późniejszej analizy i wzmacniania zabezpieczeń.

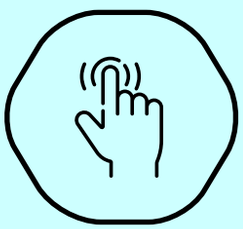
Wszystko to, za sprawą integracji szeregu narzędzi klasy **SIEM, UEBA** oraz **TDIR.**

Korzystanie z oddzielnych narzędzi nie wyeliminuje problemów w kontekście cyberbezpieczeństwa.

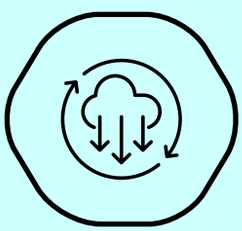
Takie struktury są uważane za zintegrowane, jednak często nie tworzą całości.

Co wyróżnia Logsign?

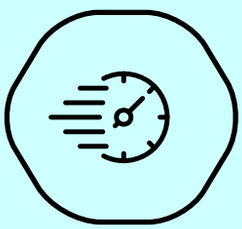
Jednolita, zintegrowana platforma



Łatwość użytkowania



Bezproblemowe wdrożenie



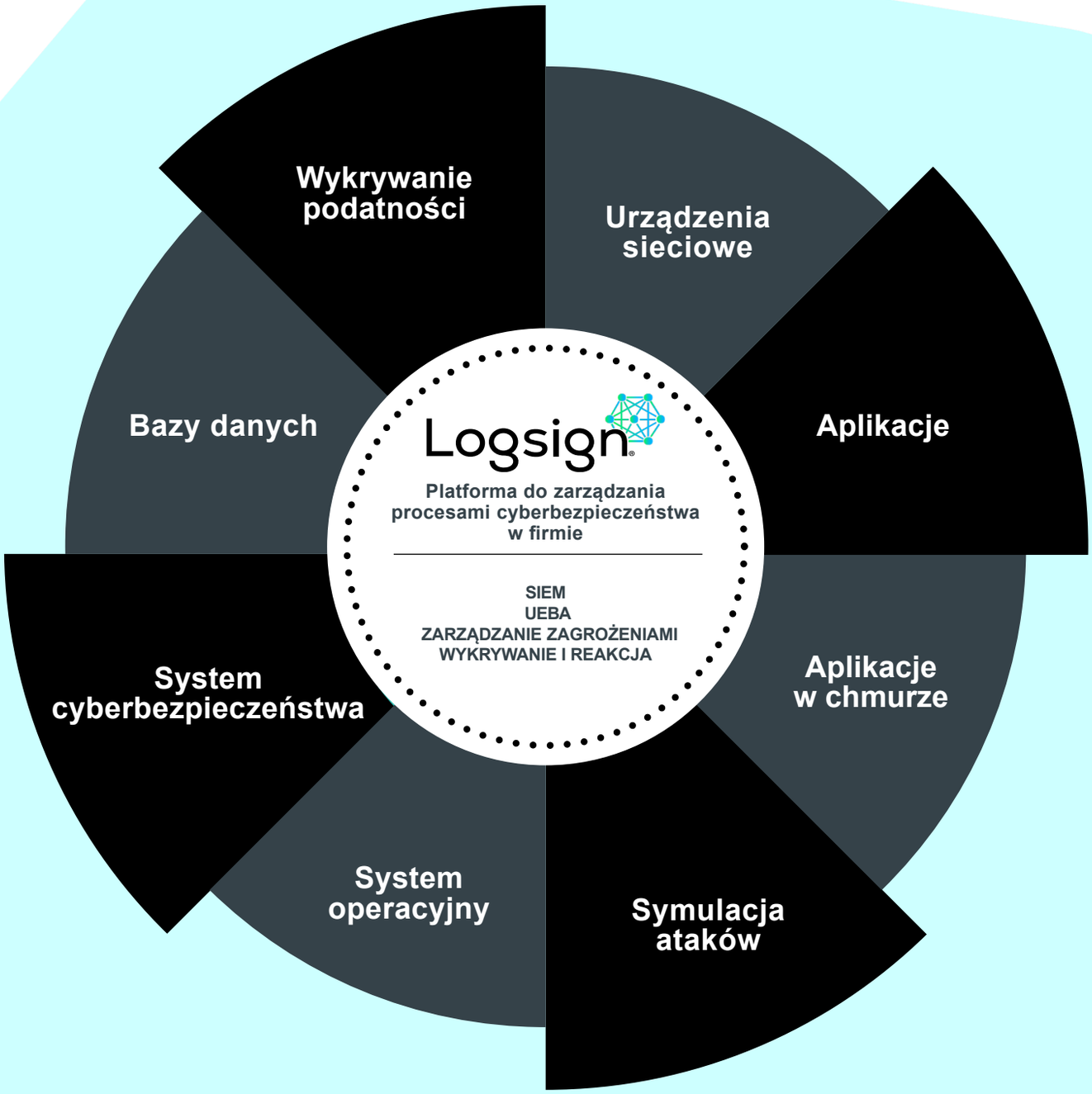
Szybkość wyszukiwania danych

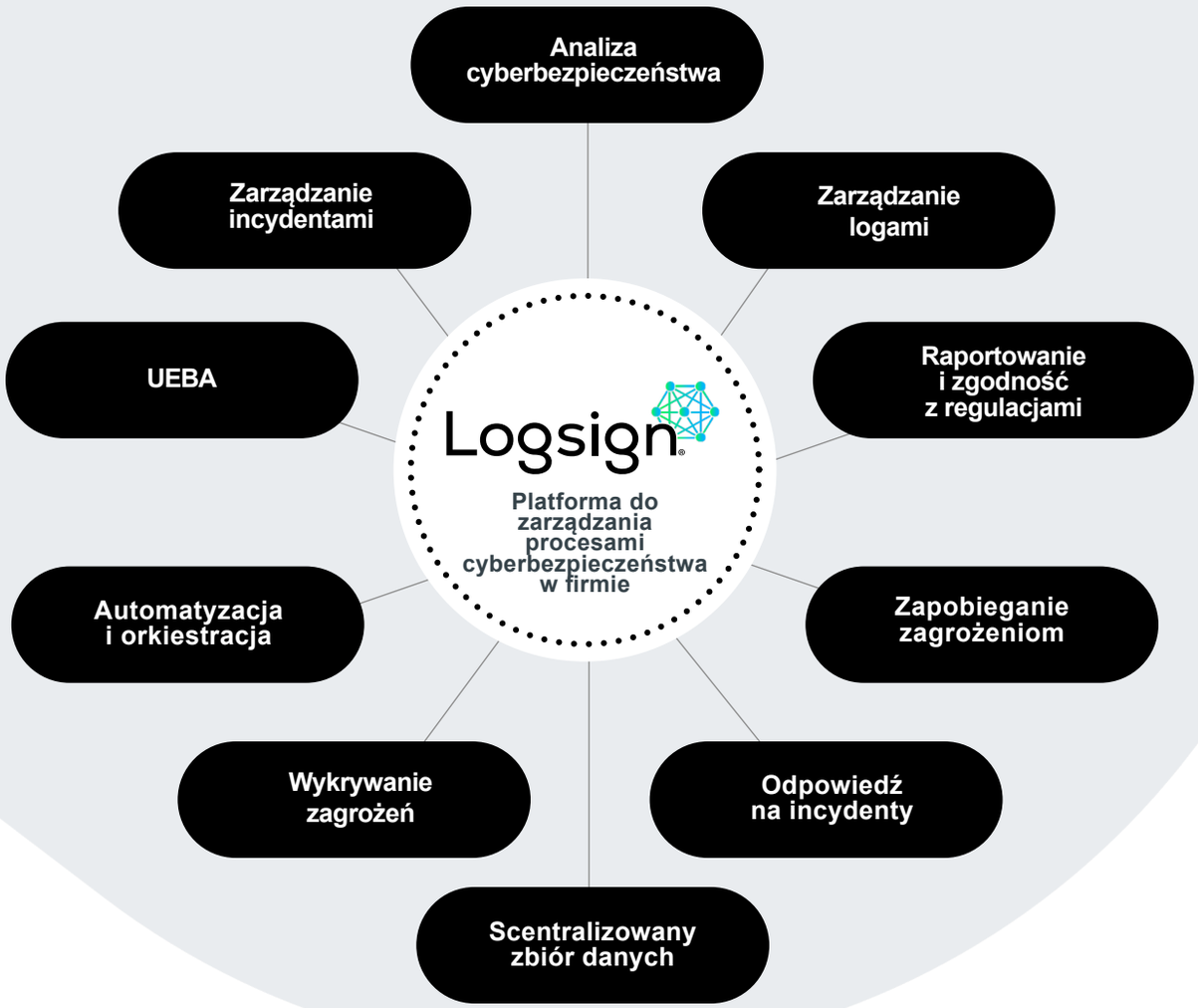
Brak ukrytych kosztów, skalowalny schemat wdrożenia

Jak działa platforma Logsign?

Logsign to wszechstronne narzędzie, które w czasie rzeczywistym wykryje cyberzagrożenia w Twojej firmie i natychmiast Cię o tym powiadomi.

Z funkcji automatyzacji i orkiestracji możesz korzystać w Logsign za sprawą modułu SOAR. Możliwości te wykorzystywane są na każdym etapie wykrywania oraz badania zagrożeń. Pozwala to na ich eliminację w ciągu zaledwie kilku sekund.





Logsign bezproblemowo integruje się ze wszystkimi niezbędnymi narzędziami SOC, aby zapewnić efektywny przepływ pracy w zespołach ds. bezpieczeństwa IT. Rozwiązanie posiada rozbudowaną bibliotekę z ponad 500 wstępnie zdefiniowanymi integracjami, bezpłatnymi bibliotekami oraz wtyczkami.

Integracje Logsign

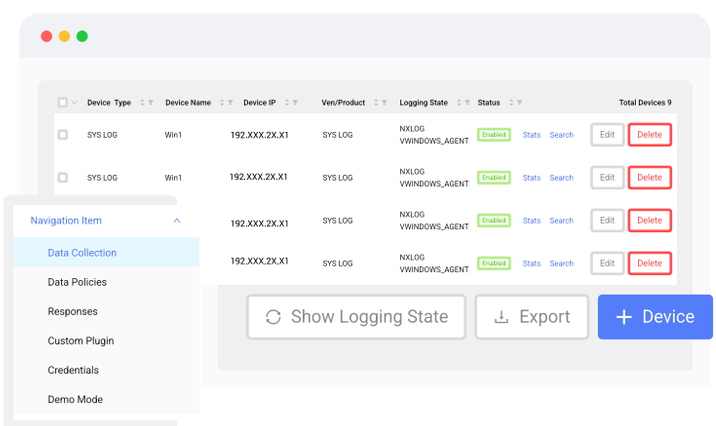
Twórz scentralizowany zbiór danych - Data Lake

Logsign zbiera dane ze wszystkich źródeł, aby stworzyć Data Lake, a następnie pracuje na zbiorze. Kluczowym czynnikiem jest tu architektura, która umożliwia:

- → Pionowa i pozioma skalowalność, na miarę architektury enterprise
- → Wdrożenie oparte na klastrach, wysoka dostępność
- → Długoterminowe przechowywanie danych
- → Zaawansowane przechowywanie wrażliwych informacji
- → Szybkie i proste wdrożenie w środowiskach hybrydowych
- → Proste i intuicyjne zarządzanie danymi gromadzonymi na co dzień w systemach firmy
- → Filtracja, indeksacja oraz strukturyzacja danych
- → Tryb demo: symulacja generowania dziennika aktywności.

Zarządzanie logami i dziennikami aktywności

Logsign zbiera dane ze wszystkich źródeł i zakątków infrastruktury IT Twojej firmy. Dzieje się tak za sprawą ponad 500 integracji z produktami różnych producentów, związanych z bezpieczeństwem oraz zgodnością z przepisami. Zarządzanie dziennikami aktywności z Logsign to:

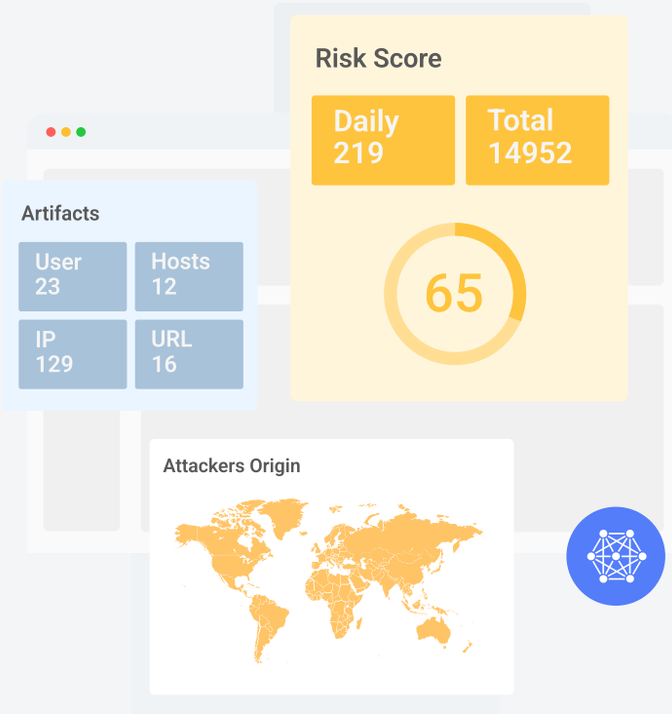


- → Ponad 400 predefiniowanych integracji z narzędziami gromadzącymi dane
- → Ponad 100 predefiniowanych integracji z narzędziami wykrywającymi i reagującymi na cyberzagrożenia
- → Bezpłatne wtyczki ułatwiające zarządzanie dziennikami aktywności
- → Zaawansowane techniki indeksacji i analizy
- → Ława praca ze znormalizowanymi i odpowiednio sklasyfikowanymi danymi
- → Bezinwazyjna modyfikacja danych
- → Wiele technik przechwytywania danych: API, NetFlow, WMI, Syslog, Oracle, SFTP, FTP, SQL, SMB, JDBC

Wykrywanie i badanie cyberzagrożeń

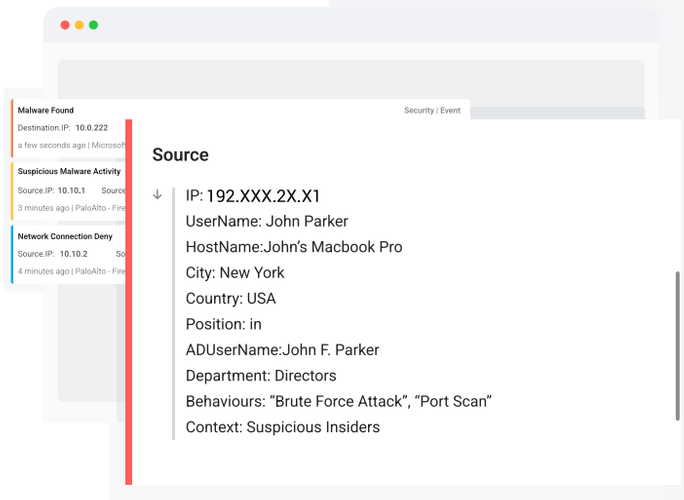
Możesz utworzyć dowolne zapytanie do bazy, aby natychmiast uzyskać potrzebne dane i informacje o incydencie. Dzięki Logsign, czas wykrycia i reakcji na incydent ograniczony jest do minimum. Jak to działa?

- → Szczegółowe, zaawansowane wyszukiwanie potrzebnych informacji
- → Odpowiedzi na zapytania w ciągu milisekund
- → Badanie skorelowanych danych
- → „Polowanie” na zagrożenia IOC i IOA
- → Walidacja poziomu zagrożenia
- → Selekcja incydentów
- → Dochodzenie kryminalistyczne
- → Frameworki: Mitre ATT@CK, Cyber Kill Chain
- → Ocena ryzyka



Działanie w czasie rzeczywistym i zaawansowana korelacja danych

Logsign wzbogaca dane i koreluje na wiele sposobów, aby zapobiegać najbardziej złożonym i nieoczywistym cyberzagrożeniom. Proces wykrywania zagrożeń odbywa się z wykorzystaniem frameworka Mitre Att@ck.



Dane wzbogacane są o:

- → Aktywa i tożsamości
- → Lokalizację, Geo IP i LDAP/AD
- → Kontekst i niestandardowe wzbogacenie danych
- → Zachowania, aktywności i zdarzenia
- → Zewnętrzne źródła informacji o zagrożeniach
- → Pozycję sieciową, umiejscowienie itp.

W kwestii korelacji:

- → Wiele technik korelacji: korelacja wzajemna, korelacja historii, oparta na regułach, oparta na zachowaniu, oparta na podatności, oparta na zagrożeniach
- → Ponad 500 predefiniowanych zasad korelacji
- → Wbudowane korelacje dla zagrożeń

Analiza zagrożeń

Logsign gromadzi wszystkie dane, wzbogaca je i porównuje z informacjami o zagrożeniach a dzięki strumieniowemu przesyłaniu informacji w czasie rzeczywistym. Podejrzane działania są więc wykrywane w najkrótszym możliwym czasie.

Logsign szybko bada ukryte zagrożenia, IOC i podejrzane wektory ataków, łącząc globalne dane o zagrożeniach. Wykorzystuje również wewnętrzne źródła zagrożeń do ustalania priorytetów ryzyka.

Narzędzie oferuje funkcje do analizy oraz wizualizacji incydentów za sprawą pulpitów nawigacyjnych.

Zaufane źródła Threat Intelligence (TI) wzbogacają dane i zapewniają wgląd w wykrywanie zagrożeń i ataków.

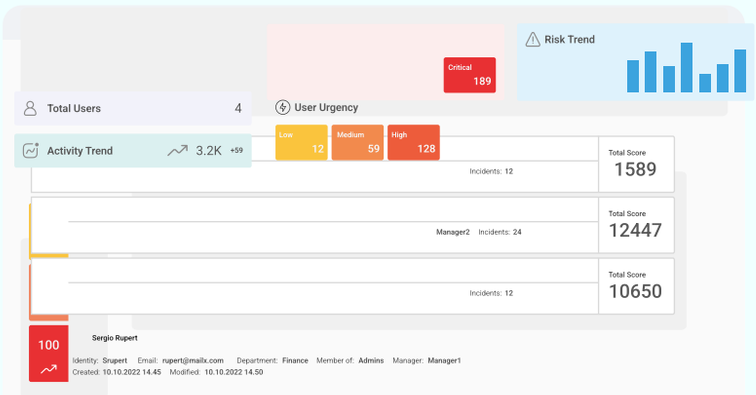
40+

Zaufanych źródeł pozwalających na wzbogacanie danych, wykrywanie zagrożeń oraz ataków.

Analiza zachowań użytkowników (UEBA)

Logsign wykorzystuje zaawansowaną technologię **UEBA** do analizy zachowań użytkowników i powiadamiania ich o potencjalnych zagrożeniach.

Aktywności użytkowników są analizowane pod kątem wykrycia typowych, ryzykownych zachowań, które mogą świadczyć o potencjalnie szkodliwych działaniach.



- → Precyzyjne wykrywanie zaawansowanych zagrożeń wewnętrznych i zewnętrznych
- → Wykrywanie alertów o najwyższym ryzyku oraz nadawanie priorytetów zagrożeniom o niskim i powolnym działaniu
- → Priorytetyzacja zagrożeń wysokiego ryzyka za pomocą analizy zachowań zorientowanej na tożsamość, która odnosi się do frameworka MITRE ATT&CK.
- → Zapobieganie i zatrzymywanie złośliwych ataków ze strony wewnętrznych użytkowników za pomocą zaawansowanej analizy zachowań od Logsign
- → Monitorowanie dostępu użytkowników do danych krytycznych
- → Zapobieganie zajęciu sieci przez botnety
- → Wykrywanie i monitorowanie podejrzanych zachowań użytkowników
- → Analiza i monitorowanie danych w czasie rzeczywistym
- → Zapobieganie wyciekom danych

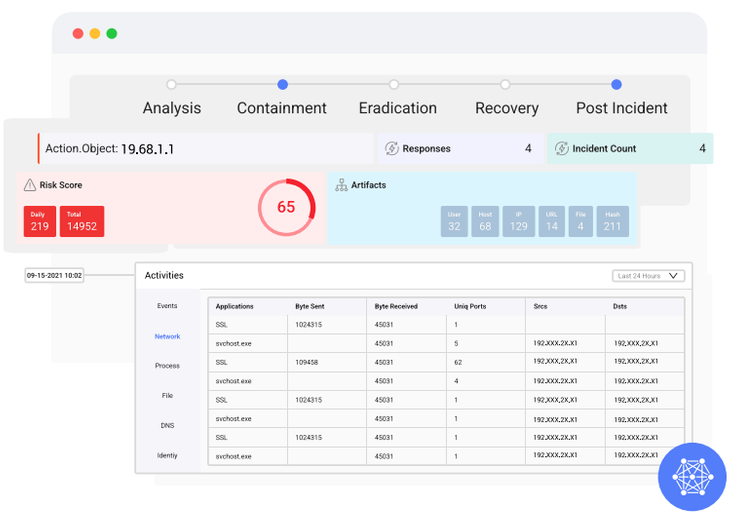
Analizy cyberbezpieczeństwa

Logsign oferuje wizualizację ataków zorientowaną na analizę bezpieczeństwa. Odbywa się to za pomocą setek predefiniowanych narzędzi.

- → Setki wbudowanych widgetów, alertów, dashboardów oraz raportów pozwalają dostarczyć konkretne wnioski przy pomocy kreatora
- → Łatwe do spersonalizowania i skonfigurowania dashboardy i widgety
- → Wielofunkcyjny kreator
- → Kontrola dostępu oparta na rolach
- → Dynamiczne filtrowanie oraz szczegółowe wyszukiwanie w dashboardach
- → Filtrowanie dashboardów w wybranym przedziale czasowym

Zarządzanie incydentami

Zarządzanie incydentami w Logsign oparte jest na cyklu życia incydentu, zalecanego przez organizację NIST. Dzięki Logsign zawsze wiesz, w której fazie cyklu znajduje się podejmowane w razie incydentu działanie.

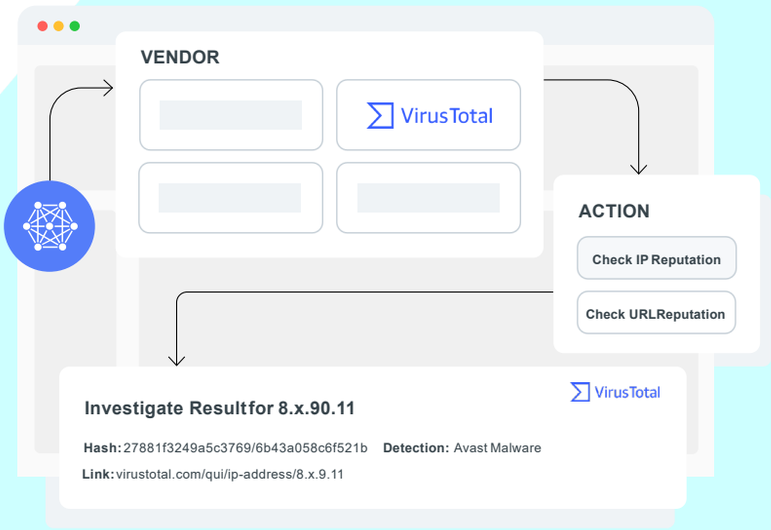


- → Zarządzanie aktywami, tożsamością i podejrzanymi aktywnościami
- → Chronologiczna prezentacja incydentu
- → Proces zarządzania incydentem zgodny z zaleceniami NIST
- → Podsumowanie zdarzeń oraz szczegółowe widoki
- → Reprezentacja graficzna zdarzeń wspomagająca analizę, wykrywanie oraz reagowanie

Natychmiastowa reakcja na incydenty

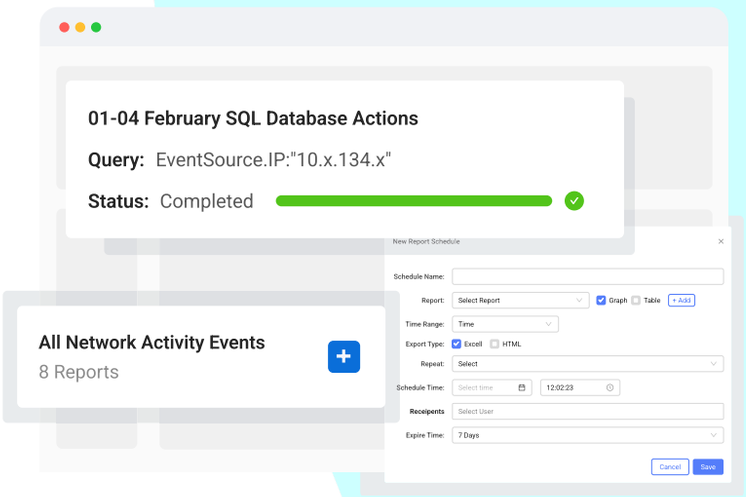
Proaktywne podejście do reakcji na incydenty w infrastrukturze IT Twojego przedsiębiorstwa.

- **Automatyzacja procesów związanych z cyberbezpieczeństwem** - dzięki temu reakcja na potencjalne zagrożenie jest natychmiastowa.
- **Półautomatyzacja** - niektóre procesy cyberbezpieczeństwa wymagają ręcznych działań, nawet po automatycznych interwencjach. Logsign, mimo automatyzacji, pozwala na zarządzanie pojedynczymi incydentami w zależności od potrzeb.



Raportowanie i zgodność z regulacjami

Logsign zapewnia zgodność z takimi regulacjami jak: **RODO, ISO/IEC 27001, NIS2, DORA**, itd.



- Setki wbudowanych szablonów raportów
- Możliwość tworzenia i konfiguracji własnych szablonów
- Eksport dokumentów w kilka sekund
- Wbudowane raporty zgodności
- Automatyzacja procesu zarządzania raportami
- Dostęp oparty na rolach

Easiest To Use SPRING 2023 · High Performer SPRING 2023 · Easiest Setup SPRING 2023 · CYBER SECURITY EXCELLENCE AWARDS WINNER 2020 · 2021 GLOBE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS · GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Logsign **Logsign Reviews**
in Security Information and Event Management
4.4
Products: Logsign Next-Gen SIEM

SECURIVY

Dowiedz się więcej:
ul. Gąsiorowskich 4B/99
60-704 Poznań
biuro@securivy.com
tel. +48 573 568 234

Znajdź nas na:

→ logsign.com → support.logsign.net