ENERGY LOGSERVER

SIEM bez limitów

Innowacyjny system do zbierania i analizy danych:
czym jest i do czego jest potrzebny?

Jakie zadania i problemy może mieć firma?

Cyfryzacja zwiększyła efektywność wielu procesów, ale też przyczyniła się do powstania kilku nowych kwestii:

Dane elektroniczne są łatwiejsze do przetwarzania,

ALE

są teraz celem konkurencji i przestępców.

Klientów łatwiej znaleźć dzięki aplikacjom mobilnym,

ALE

musisz polegać na stabilnym działaniu tych aplikacji.

Sieci korporacyjne i usługi chmurowe optymalizują pracę pracowników,

ALE

ich porażka paraliżuje organizację.

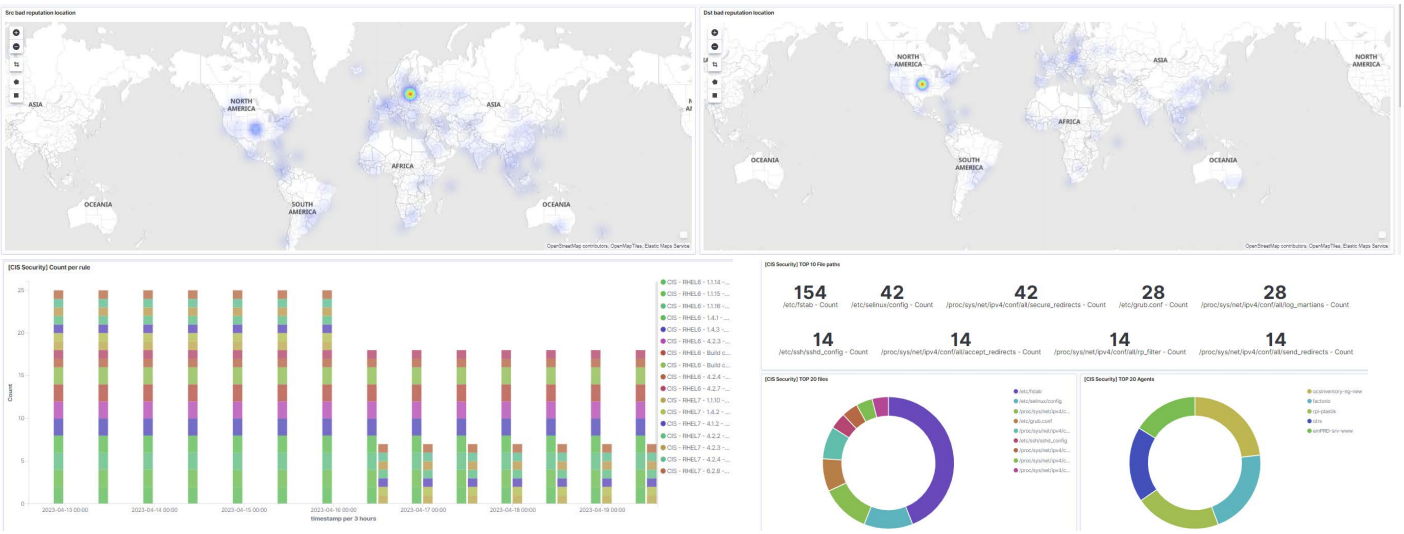
Innymi słowy, firmy stają się bezpośrednio uzależnione od efektywności cyberbezpieczeństwa i jakości obsługi systemów informatycznych.

Konieczne jest gromadzenie oraz analizowanie terabajtów informacji o zagrożeniach, zdarzeniach związanych z bezpieczeństwem, stanie sprzętu, strukturze ruchu i innych metrykach, aby móc wykryć ataki na czas i utrzymać dostępność usług.

System SIEM dobrze wpasowuje się w opis tych zadań, ale dowolnego rozwiązania dostępnego na rynku może okazać się niewydajne.

Wybierając rozwiązanie, można napotkać wiele problemów, takich jak niewystarczająca moc, a także niewystarczające integracje z obecnymi systemami, brak zasobów pamięci masowej i wiele innych.

Jedynym sposobem rozwiązania tego problemu jest usunięcie wszystkich ograniczeń.



Energy Logserver: SIEM, który wychodzi poza schemat

Może wyglądać jak klasyczny SIEM z typową logiką – integrować się z twoimi systemami, zbierać oraz przechowywać dzienniki zdarzeń systemowych, normalizować i korelować logi oraz analizować ruch sieciowy. Ale to tylko na papierze.

W praktyce twórcy rozwiązania dopracowali każdą funkcję do perfekcji. Możesz zbierać logi bez limitów EPS i przestrzeni dyskowej oraz integrować je ze wszystkimi niezbędnymi rozwiązaniami, dzięki czemu nie stracisz ani jednego bajta kluczowych danych.

Przejdźmy do bardziej szczegółowych informacji na temat funkcji Energy Logserver.

Energy Logserver: kluczowe cechy

Log management oraz SIEM

Dane kontrolują wszystko w nowoczesnym biznesie. Specjaliści potrzebują terabajtów logów z różnych systemów, aby zapewnić kontrolę i bezpieczeństwo sieci. Ręczne przetwarzanie tak dużej ilości danych jest niemożliwe - do tego właśnie służy SIEM Energy Logserver, który umożliwia zbieranie, przechowywanie i przetwarzanie informacji z różnych źródeł, analizowanie i korelowanie zdarzeń oraz wyciąganie wniosków, które pomagają podejmować skuteczne decyzje operacyjne.

Monitorowanie infrastruktury

Infrastruktura staje się coraz bardziej złożona, a jej elementy wymieniają dane o swoim stanie za pomocą różnych protokołów. Energy Logserver może śledzić trendy oraz wskaźniki, aby zapewnić holistyczne informacje o stanie Twojej sieci.

Monitorowanie wydajności aplikacji

Aplikacje są krytycznym aspektem biznesowym dla każdej organizacji. Z tego powodu są celem przestępców. Energy Logserver pomaga śledzić wskaźniki, transakcje, błędy, awarie i inne procesy wewnętrzne w celu szybkiego wykrywania i eliminowania problemów.

Monitorowanie chmury

Dzięki chmurze organizacje skracają czas potrzebny do wprowadzania nowych produktów i czynią je bardziej elastycznymi. Jednocześnie chmura zapewnia mniejszą widoczność procesów, kontrolę nad danymi i bezpieczeństwo.

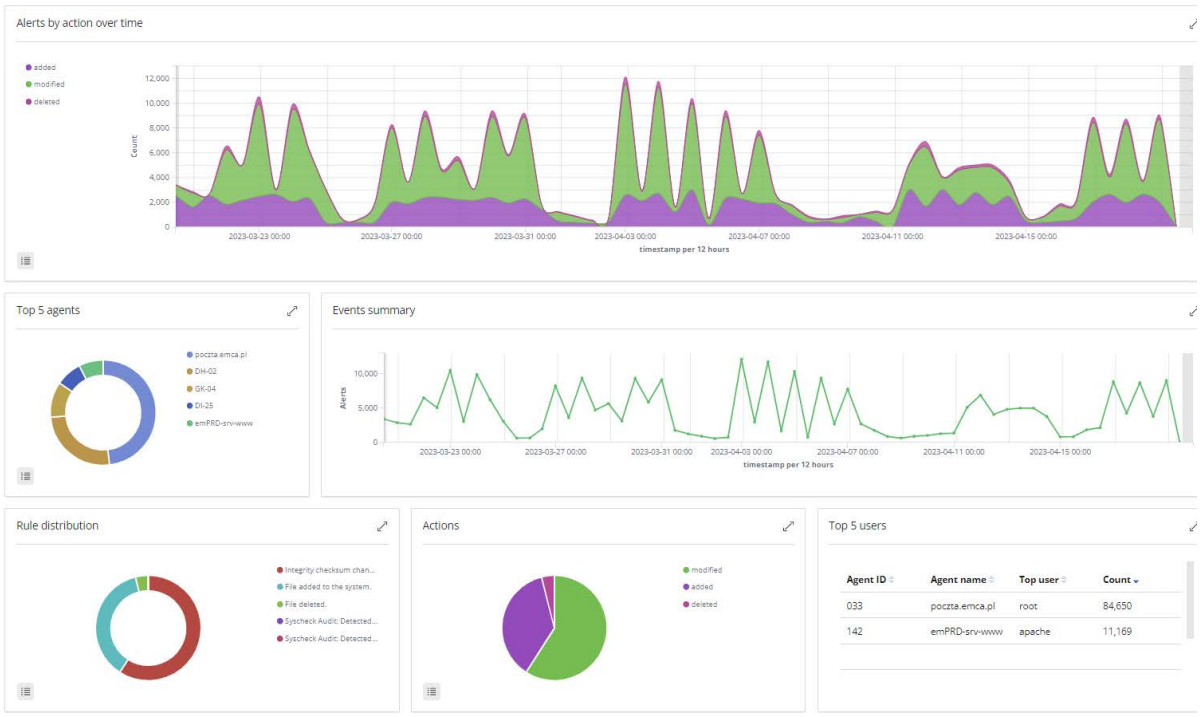
Integracja z AWS i Azure pozwala wyróżnić i zobaczyć parametry EC2, RDS, AMI, S3 i IAM oraz poprawić kontrolę nad chmurą.

Zgodność z regulacjami

Compliance to stosowanie skutecznych rozwiązań i ustalanie odpowiednio wysokiego poziomu bezpieczeństwa danych, zgodnie z dokumentami, regulacyjnymi oraz międzynarodowymi standardami. Są one obowiązkowe dla wszystkich firm, których dotyczą. Energy Logserver pomaga zachować zgodność z RODO, PCI-DSS, NIST 800-53, HIPAA, NIS 2 i ISO 27001.

Integracja z MITRE ATT&CK

MITRE ATT&CK to globalnie dostępna baza metod i taktyk cyberataków stworzona na podstawie rzeczywistych incydentów.



Energy Logserver wykorzystuje tę bibliotekę do pozyskiwania dodatkowych danych do wykrywania incydentów bezpieczeństwa, dzięki czemu wszelkie podejrzane zdarzenia mogą być natychmiast porównywane z bazami danych naruszeń i oznaczane jako zagrożenie.

Analiza ruchu

Ruch sieciowy jest dodatkowym źródłem informacji o wykrywaniu incydentów bezpieczeństwa.

Energy Logserver porównuje logi z informacjami o pakietach danych, aby zapewnić analizę oraz umożliwić specjalistom ds. bezpieczeństwa reagowanie na ataki na czas.

Analiza bezpieczeństwa

Informacje o konfiguracjach oprogramowania i sprzętu, istniejące zagrożenia i inne incydenty są kluczem do kontroli poziomu bezpieczeństwa.

Dziesiątki rozwiązań monitorują różne elementy bezpieczeństwa, ale potrzebny jest tzw. widok z lotu ptaka na cały jego stan. Energy Logserver zapewnia niezbędną funkcjonalność do porównywania danych, a także zrozumienia aktualnych zagrożeń i kroków, aby im przeciwdziałać.

Dlaczego wybrać Energy Logserver?

Energy Logserver usuwa wszystkie typowe ograniczenia, takie jak:

Wydajność	Elastyczność	Ilość danych	Skalowalność	Zadania i obszary zastosowania
Wysoka wydajność na pojedynczym data node - do 5000 EPS. Brak ograniczeń objętości danych.	Setki integracji pozwalają na zbieranie danych z praktycznie dowolnego źródła, bez ograniczeń i kompromisów.	Nieograniczona ilość źródeł danych, ich rodzajów i wolumenu.	Możliwość rozszerzenia rozwiązania o kolejne data node zwiększając przy tym możliwości platformy.	Energy Logserver świetnie sprawdza się w firmach z różnych sektorów i rozwiązuje zadania nietypowe dla platformy SIEM.

ENERGY LOGSERVER

Przegląd kluczowych cech:

- Elastyczna architektura i prosta skalowalność dzięki dodawaniu węzłów do klastra
- Integracja z dowolnymi systemami
- Analiza środowisk chmurowych
- Analiza wydajności sieci i aplikacji
- Nieograniczona liczba źródeł danych, użytkowników

Energy Logserver - przykłady użycia

Energy Logserver sprawdzi się we wszystkich firmach, zadaniach i dziedzinach. Ale korzystanie ze wszystkich funkcji nie zawsze jest konieczne - możesz potrzebować rozwiązania do oddzielnych zadań w określonych kategoriach. Masz trzy możliwości wykorzystania Energy Logserver.

Log Management: wszystko o zarządzaniu dziennikami zdarzeń

Centralizacja zdarzeń oraz gromadzenie dokumentów to kluczowe zadania Energy Logserver. Stanowią one podstawowy moduł rozwiązania. Dzięki niemu masz możliwość zbierania logów w celu analizy, przeglądania zapisów pamięci oraz kontroli procesów bezpieczeństwa.

- Zarządzanie użytkownikami, RBAC
- Integracja z LDAP, AD, Radius, SSO
- Skalowalna architektura i tworzenie klastrów
- Setki gotowych parserów
- System powiadamiania i raportowania
- Wielopoziomowy system archiwizacji danych
- Gotowe dashboardy i szablony

SIEM: rozszerzone zarządzanie bezpieczeństwem

Gromadzenie i korelacja danych, kompleksowe zrozumienie stanu bezpieczeństwa, istniejących zagrożeń, luk w zabezpieczeniach, problemów z konfiguracją itp.

- Analiza behawioralna użytkowników i urządzeń
- Dynamiczna integracja z bazami danych IoC, TTP, Threat Intelligence, MITRE ATT&CK
- Zgodność z RODO, NIST, CIS, PCI DSS, HIPAA
- Monitorowanie integralności plików (FIM)
- Skanowanie podatności
- Ponad 1000 reguł wykrywania i korelacji
- Pomoc sztucznej inteligencji w wykrywaniu podejrzanych zachowań
- Playbooki
- Monitorowanie aplikacji i usług
- Zintegrowany system zarządzania ryzykiem
- System zarządzania incydentami

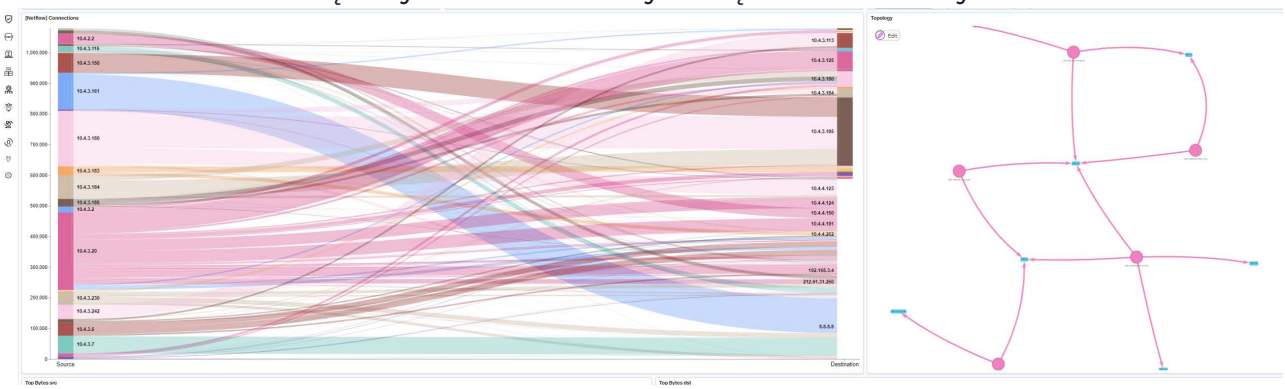
Network Probe: Analiza sieci

Zbieranie danych o ruchu sieciowym, sprzęcie, stanie infrastruktury i wszystkim co jest związane z ruchem w Twojej sieci.

- Szczegółowa analiza ruchu sieciowego
- Analiza Netflow (v5, v9, IPFIX, sflow. jflow. NetStream)
- Wydajność od 10 Gb/s
- Od 100 000 FPS
- Wizualizacja ruchu w warstwie L2-L7
- Korelacja logów i danych o ruchu
- Kontrola ruchu zgodnie z bazami danych reputacji i IoC
- Wykrywanie ataków zero-day
- Analiza aktywności sieciowej użytkowników
- Monitorowanie SRT, RTT, Delay, Jitter, anomalii sieciowych

Dane to podstawa każdej organizacji, umiejętność ich gromadzenia i analizowania — klucz do efektywnych procesów biznesowych.

Dane są wszystkim. Pomożemy Ci mądrze z nich korzystać.



Miej wszystkie dane w zasięgu wzroku dzięki Energy Logserver! Skontaktuj się z nami, korzystając z poniższych danych, skonsultuj się z naszymi inżynierami i zamów wersję próbną.

InfoProtector Sp. z o.o.

ul. Wł. Żeleńskiego 103, 31-353 Kraków

infoprotector@infoprotector.pl

tel. 12 350 26 62

Dowiedz się więcej:

Energy Logserver to firma, która produkuje rozwiązania SIEM i SOAR do gromadzenia i analizowania zapisów logów i zdarzeń związanych z cyberbezpieczeństwem. Produkty firmy spełniają zadanie centralizacji zarządzania SI, upraszczają procesy i zwiększają efektywność działów IT.

Więcej informacji: www.energylogserver.com

Firma InfoProtector powstała w odpowiedzi na rosnące zapotrzebowanie nowych, często unikalnych rozwiązań minimalizujących ryzyko utraty danych. Dostarczamy rozwiązania i usługi z obszarów bezpieczeństwa sieci, serwerów, stacji roboczych, urządzeń mobilnych oraz dostępu fizycznego. Koncentrujemy się na doborze odpowiednich rozwiązań będących odpowiedzą na wyzwania naszych klientów.

Więcej informacji www.infoprotector.pl