STORMSHIELD

ROZWIĄZANIE DO ZARZĄDZANIA LOGAMI

# STORMSHIELD
# LOG SUPERVISOR

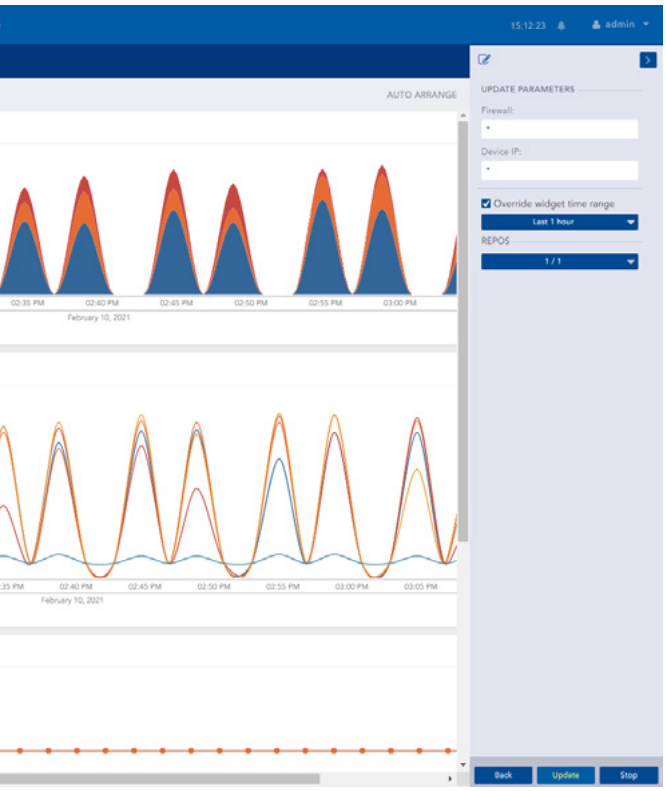
Popraw jakość gromadzonych danych

**ZAAWANSOWANA**
ANALIZA LOGÓW

**ZGODNOŚĆ**
DZIĘKI ARCHIWIZACJI DANYCH

**RAPORTY**
RĘCZNE I AUTOMATYCZNE

**CENTRALNE**
ZARZĄDZANIE LOGAMI




## Zadbaj o cyberbezpieczeństwo dzięki monitorowaniu

Każdego dnia na świecie pojawiają się coraz bardziej zaawansowane zagrożenia, w związku z czym dokładne monitorowanie danych staje się nieodzowne. Rozwiązanie Stormshield Log Supervisor (SLS) zapewnia lepszy wgląd w logi sieciowe, jednocześnie umożliwiając administratorom dostosowanie i optymalizację reakcji na incydenty.

### Pełna widoczność

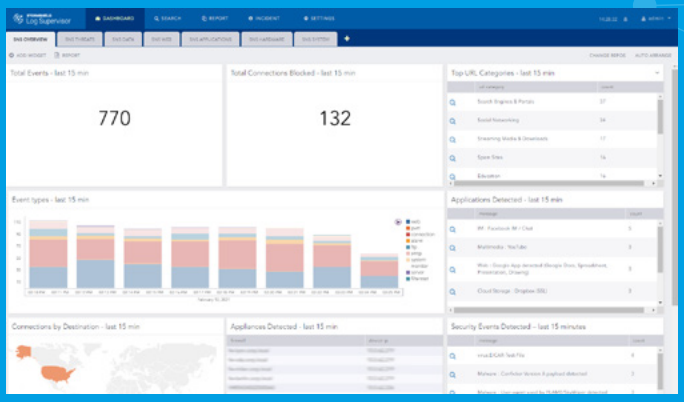
- Wizualizacje, sprawozdania, alerty.
- Wyszukiwanie na podstawie wielu kryteriów.
- Raporty dotyczące aktywności.
- Łatwe wyszukiwanie i prosta składnia.

### Skalowalność

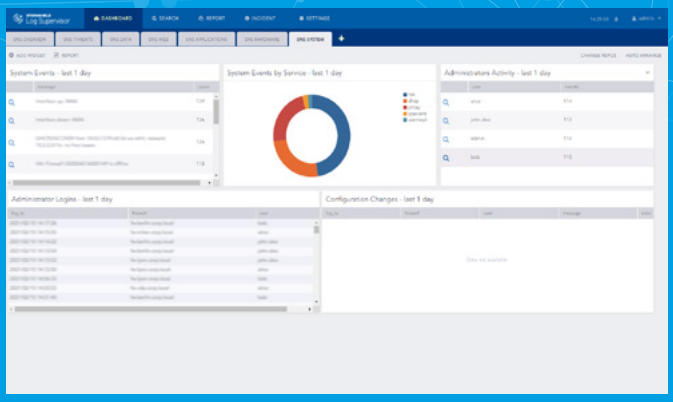
- Obsługa wielu urządzeń.
- Zarządzanie dużą ilością logów na przestrzeni lat.
- Wysoka dostępność.

### Zarządzanie incydentami

- Tworzenie reguł dla wyzwalanych alertów.
- Zarządzanie alertami i incydentami.

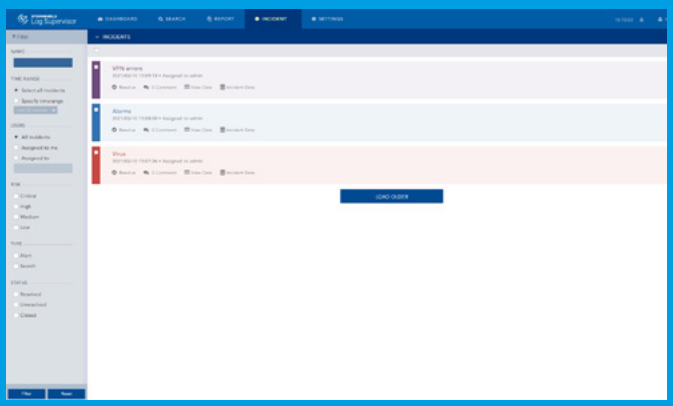



Widok SLS



Podgląd zdarzeń systemowych

Wyszukiwarka logów



Alerty

## LISTA FUNKCJI

### *ZARZĄDZANIE LOGAMI*

- Gromadzenie zdarzeń przez syslog (TCP oraz UDP)
- Bezpieczne gromadzenie danych przez syslog-TLS
- Syslog Forwarder
- Liczba zdarzeń na sekundę (EPS): > 10 000
- Normalizacja i natywne indeksowanie logów SNS
- Zarządzanie logami przez wiele lat (> 1 roku)
- Liczba urządzeń > 500

### *RODZAJE WYSZUKIWAŃ*

- Wyszukiwanie proste
- Wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.)
- Wyszukiwanie predefiniowane
- Rezultaty wyświetlane jako logi proste, znormalizowane i graficzne
- Możliwość wykorzystania zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP)
- Nawigacja na podstawie czasu (minut, godzin, dni, okresów)
- Historia wyszukiwania
- Eksport wyników w formacie CSV

### *PANELE KONTROLNE*

- Widoki ogólne (zagrożenia, dane, aplikacje internetowe, sprzęt i system)
- Możliwość dostosowania istniejących widgetów
- Możliwość tworzenia nowych widgetów
- Ponad 20 rodzajów widoków graficznych (histogramy, radary, mapy, itd.)

### *ZARZĄDZANIE INCYDENTAMI I ALERTAMI*

- Automatyczne generowanie na podstawie ustalonych reguł
- Zarządzanie krytycznością alertów na 4 poziomach krytyczności
- Możliwość przypisania incydentów do administratorów i śledzenie rozwiązania

### *RAPORTY*

- Ręczne lub automatyczne (godzinne, dzienne, tygodniowe lub miesięczne)
- Możliwość dostosowania układu
- Formaty raportów: PDF, HTML, XLS, DOCX, CSV
- Możliwość wysyłania raportów mailem

### *KOMPATYBILNOŚĆ*

Hiperwizory:

- VMWare ESXi 6.5 oraz 7
- Microsoft HyperV: Windows Server 2016

Produkty Stormshield:

| Produkt | Od wersji |
|---|---|
| SNS | 3.7.X |