mediafon TECHNOLOGY

SOC as a Service od Mediafon Technology

Oberig it Europe

Globalne zagrożenia i wyzwania

CO DRUGA FIRMA

na świecie zostanie dotknięta cyberatakiem w 2025 r.* Prognozowane straty sięgną ponad 10 bilionów dolarów.

€4.1 MILIONA

średni koszt wycieku danych dla firm i organizacji

80%–95% luk w zabezpieczeniach wynika z błędów LUDZKICH

95% cyberataków ma czynnik ludzki**

WYŻSZE KOSZTY UBEZPIECZENIA

dla firm, które nie mają odpowiednich strategii cyberbezpieczeństwa

12–36 MIESIĘCY

czas potrzebny do stworzenia w pełni operacyjnego wewnętrznego zespołu cyberbezpieczeństwa

*Cybersecurity report 2022 by Gartner

** The Global Risks Report 2022 by the World Economic Forum

Kluczowe biznesowe wyzwania

- 75% wzrost liczby cyberataków w ciągu ostatnich 5 lat przewiduje się, że do 2025 r. przekroczy 10 bilionów dolarów
- 40%–70% poszkodowanych firm to małe przedsiębiorstwa
- Rosnąca zależność od IT i technologii w celu zapewnienia ciągłości działania
- Niski poziom rozwoju IT w firmach z sektora MŚP
- Brak wykwalifikowanych specjalistów i wysokie koszty ich zatrudnienia
- Wzrost integracji narzędzi technologicznych w organizacjach
- Wpływ nadchodzących dyrektyw: NIS2, DORA, MiCA
- Rosnące wymagania dotyczące bezpieczeństwa informacji ze strony dostawców/partnerów/instytucji

Dlaczego SOC zostało stworzone przez Mediafon Technology

Międzynarodowy dostawca usług IT i TELCO

25+
lat doświadczenia

15+
państw

400+
serwerów zarządzanych

24/7
serwis

ZGODNOŚĆ Z NORMAMI ISO:
ISO 14001:2004, ISO 9001:2008, ISO 27001:2013

- Firma MTECH – 25 lat doświadczenia w opracowywaniu, wdrażaniu i utrzymywaniu rozwiązań IT i TELCO działających na wszystkich kontynentach. Cyberbezpieczeństwo ma szczególne znaczenie dla produktów i usług, które sami opracowujemy, ponieważ od niego zależy ich funkcjonalność w wielu krajach.
- Wraz ze wzrostem znaczenia cyberbezpieczeństwa nie jest to już tylko potrzeba biznesowa — staje się ono coraz częściej wymogiem, nakazanym przez różne dyrektywy lub narzuconym przez dostawców, partnerów lub klientów. Systemy muszą być bezpieczne i chronione przed cyberzagrożeniami.
- Mediafon Technology, korzystając ze swojego doświadczenia i mając świadomość rosnącego znaczenia cyberbezpieczeństwa w różnych sektorach biznesowych, opracowało rozwiązanie SOC przeznaczone specjalnie dla małych i średnich przedsiębiorstw (MŚP), oparte na stałej komunikacji z klientami.
- Mediafon Technology SOC as a Service – rozwiązanie dla wszystkich, którzy poszukują usługi umożliwiającej proaktywne wykrywanie incydentów związanych z cyberbezpieczeństwem w infrastrukturze IT w odpowiednim czasie, bez konieczności ponoszenia dużych wydatków inwestycyjnych, opłat rocznych lub niejasnych kosztów.
- Narzędzie jest elastyczne i można je dostosować do różnych potrzeb, korzystając z 10 najlepszych globalnych rozwiązań SIEM typu open-source

SOC – jak to jest widoczne w kontekście ISMS (system zarządzania bezpieczeństwem informacji)

Centrum operacji bezpieczeństwa (SOC) – część organizacji lub usługa zewnętrzna, która dzięki wykorzystaniu specjalistów, procesów i technologii nieustannie monitoruje urządzenia i sieć organizacji w celu zapobiegania cyberzagrożeniom.

Kluczowe funkcje SOC zgodnie z ISMS:

- ✓ Monitorowanie i analiza złośliwego oprogramowania, zagrożeń wewnętrznych i cyberoszustw.
- ✓ Monitorowanie i zarządzanie podatnościami.
- ✓ Identyfikacja, ocena i rozwiązywanie incydentów.
- ✓ Regularne raporty i rekomendacje.
- ✓ Monitorowanie, wykrywanie, analiza i ocena zdarzeń związanych z bezpieczeństwem.

Czy usługa SOC oferowana przez Mediafon Technology spełnia te funkcje?

ODPOWIEDŹ: TAK – i to nie wszystko, ponieważ stajemy się również partnerem w zakresie doradztwa w zakresie cyberbezpieczeństwa.

Jak to działa:

KROK 1: PRZYGOTOWANIE

- Zaczniemy od szczegółowych konsultacji, podczas których nasi eksperci bezpieczeństwa będą ściśle współpracować z zespołem klienta, aby zrozumieć istniejącą infrastrukturę, zidentyfikować potencjalne słabe punkty i określić konkretne cele bezpieczeństwa.
- Ten etap pozwala nam dostosować usługi SOC do potrzeb biznesowych klienta. Wspólnie z klientem opracujemy plan integracji źródeł w SOC.

KROK 2: INTEGRACJA

- Łączenie źródeł z systemem SIEM (Security Information and Event Management). Wdrożenie wymaganych narzędzi systemowych.
- Konfiguracja potoków danych i zbieranie logów zdarzeń z różnych źródeł.
- Udostępnienie systemów samoobsługowych do zarządzania incydentami.

Testowanie i optymalizacja:

- Po udanym testowaniu i szkoleniu przechodzimy do rzeczywistej eksploatacji. Od tego momentu nasze centrum SOC będzie aktywnie monitorować środowisko klienta przez całą dobę, wykrywając zagrożenia i reagując na nie w czasie rzeczywistym. Regularnie dostarczamy raporty i przeprowadzamy optymalizacje, aby zapewnić bezpieczeństwo działalności klienta. Przeprowadzamy kompleksowe testy i przygotowujemy się do rzeczywistej eksploatacji, co pozwala nam precyzyjnie dostosować konfiguracje i protokoły reagowania w oparciu o rzeczywiste sytuacje.

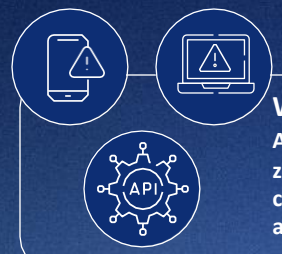
KROK 3: MONITOROWANIE

- **Uruchamianie i ciągłe monitorowanie (okres stabilizacyjny)**

KROK 4: DZIAŁANIE

Reagujemy natychmiastowo na cyberataki lub nowo wykryte zagrożenia. Organizujemy szkolenia dla zespołu klienta, aby zapewnić mu pełną gotowość do współpracy z naszym centrum SOC i wykorzystania wszystkich dostępnych narzędzi. Dostarczamy szczegółowe wskazówki i najlepsze praktyki, aby zmaksymalizować korzyści płynące z naszych usług.

1. Nasze oprogramowanie stale monitoruje logi komponentów systemu (urządzeń fizycznych, usług w chmurze itp.).
2. Wszystkie zarejestrowane zdarzenia są sprawdzane pod kątem zgodności z polityką bezpieczeństwa, dozwolonymi działaniami i standardowymi zachowaniami.
3. Po wykryciu naruszenia bezpieczeństwa, nieautoryzowanego działania lub nietypowego zachowania klient i zespół cyberbezpieczeństwa są od razu powiadamiani o problemie i zalecanych działaniach za pośrednictwem poczty elektronicznej, SMS-ów lub bezpośrednio do systemów klienta poprzez API.



WAŻNE

Automatyczne alerty są wysyłane wyłącznie w przypadku zagrożeń wysokiego ryzyka i zdarzeń określonych przez klienta. Wszystkie inne kwestie związane z cyberbezpieczeństwem są filtrowane i sprawdzane przez nasz zespół bezpieczeństwa, aby zminimalizować liczbę niepotrzebnych fałszywych alarmów.

SOC - Ciągłe wsparcie i optymalizacja

Nasze zaangażowanie nie kończy się na fazie przygotowań. Nieustannie wzmacniamy poziom bezpieczeństwa poprzez regularne aktualizacje, optymalizację systemu i ciągłą pomoc techniczną:

- Regularne aktualizacje informacji o zagrożeniach.
- Kwartalne przeglądy i optymalizacja systemu.
- Zarządzanie incydentami.
- Redukcja fałszywych alarmów i generowanie nowych alertów.

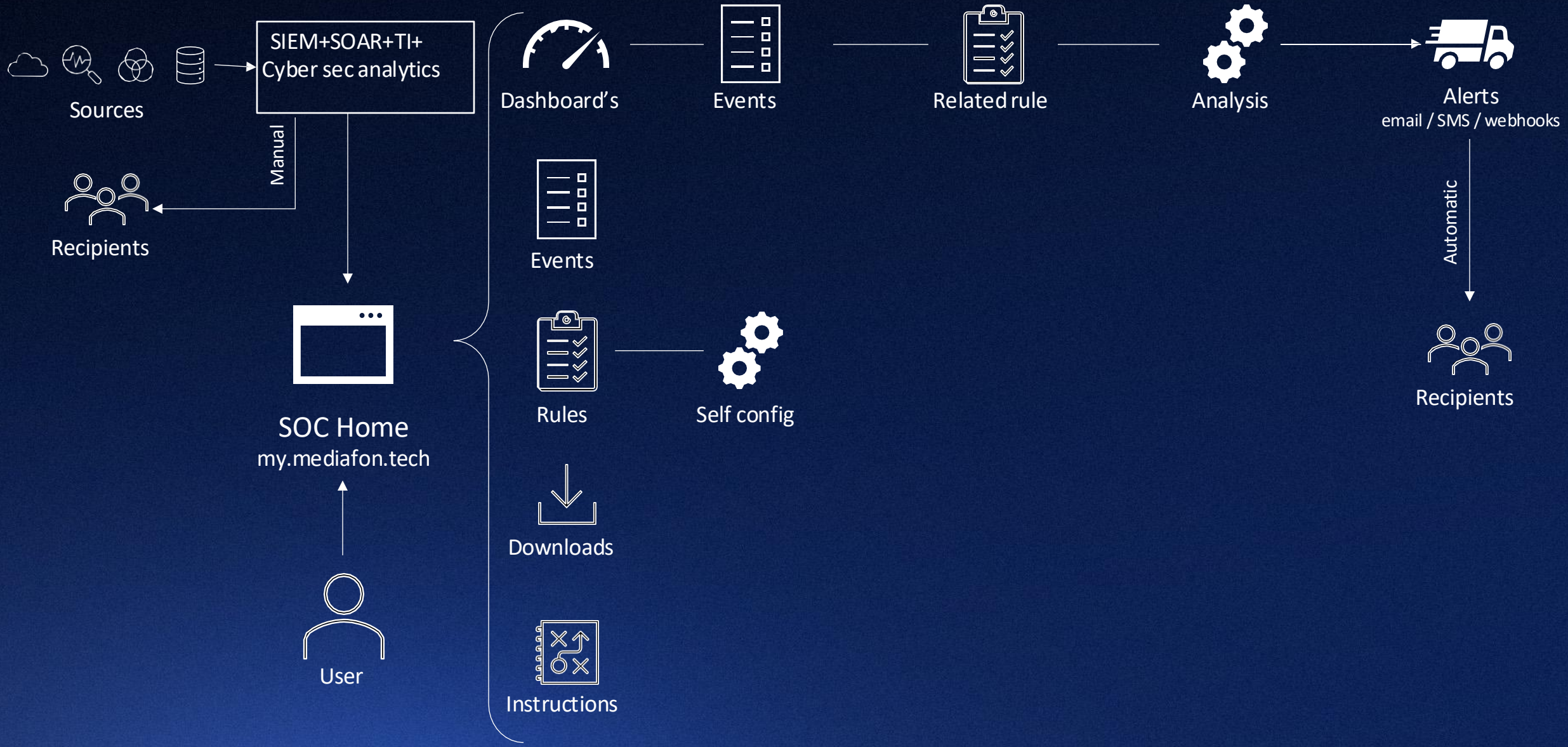
Struktura regularnych spotkań SOC

PRZEGLĄD ZDARZEŃ Z POPRZEDNIEGO MIESIĄCA	1	Krótka dyskusja na temat wydarzeń i incydentów, analiza oraz kluczowe wnioski.
PROGRES W REALIZACJI NIEUKOŃCZONYCH ZADAŃ	2	Prace zakończone i kluczowe osiągnięcia zespołu MTCH związane z SOC.
PROGRES W WYKONANIU ZADAŃ KLIENTA I ZADAŃ SKOŃCZONYCH	3	Działania po stronie klienta: działania wykonane na podstawie zaleceń SOC i ogólnych celów bezpieczeństwa.
PLANOWANIE KOLEJNYCH ZADAŃ	4	Przegląd nadchodzących zadań, w tym priorytetowych zadań określonych na podstawie potrzeb klienta i zaleceń MTCH.

SOC
Moduł techniczny

Jakich narzędzi używamy?

Schemat SOC


Sources
SIEM+SOAR+TI+
Cyber sec analytics
Manual
Recipients
SOC Home
my.mediafon.tech
User
Dashboard's
Events
Related rule
Analysis
Alerts
email / SMS / webhooks
Automatic
Recipients
Events
Rules
Self config
Downloads
Instructions

Skontaktuj się z nami!

Oberig IT Europe jest częścią grupy firm Oberig IT, działającą na europejskim rynku i specjalizującą się w dystrybucji rozwiązań VAD (Value-Added Distribution) z zakresu bezpieczeństwa informacji oraz infrastruktury IT. Dzięki doświadczonemu zespołowi certyfikowanych inżynierów oferujemy kompleksowe wsparcie na każdym etapie projektu – od konsultacji przedwdrożeniowych, przez implementację, aż po szkolenia i opracowanie dokumentacji.

https://oberig-it.eu/