smartech IT

# Strategia Cyfrowego Bezpieczeństwa |

KROK 1 | Zarządzanie dokumentacją

KROK 2 | Testy penetracyjne

KROK 3 | Skanowanie podatności

KROK 4 | Zarządzanie logami

KROK 5 | Usługi SOC

www.smartech-it.eu

# KROK 1 | Zarządzanie dokumentacją

Utrzymywanie dokumentacji według określonych standardów branżowych oraz prawnych to ważny element utrzymania odpowiedniego poziomu bezpieczeństwa firmie. W przypadku wdrożenia standardów takich jak normy ISO, wymagania prawne czy wymagania branżowe, zasady związane z dokumentacją są skomplikowane i wymagają odpowiedniej wiedzy.

## Aby osiągnąć oczekiwaną dojrzałość firmy:

nasi specjaliści **przeanalizują istniejącą dokumentację** Państwa firmy;

ocenią poziom jej dojrzałości i **wskażą braki** wymagające uzupełnienia;

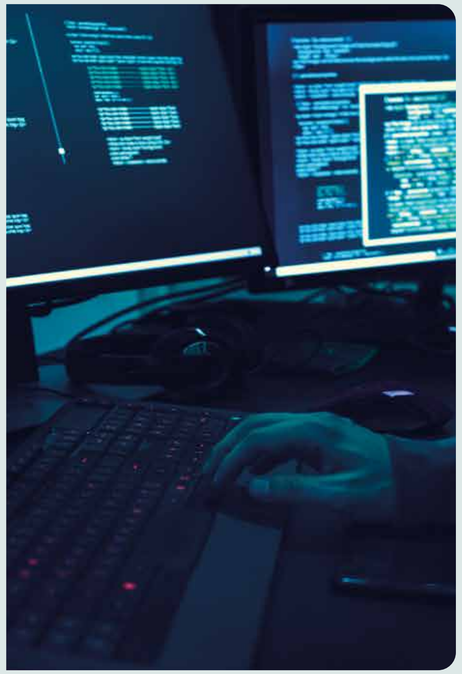
otrzymają Państwo również **konkretną listę działań**, jakie należy podjąć, aby osiągnąć pełną zgodność z obowiązującymi przepisami prawa oraz standardami;

nasz zespół skupi się również na **analizie schematów sieciowych, topologii sieci, inwentaryzacji sprzętu i oprogramowania;**

zbadamy **organizację kontroli dostępu do zasobów, kont użytkowników, ról oraz uprawnień w systemach IT** . W ten sposób gromadzimy kompleksową wiedzę na temat stanu bezpieczeństwa infrastruktury IT organizacji oraz identyfikujemy wymagające uzupełnienia braki w dokumentacji.

# KROK 2 | Testy penetracyjne

W czasach, gdy większość organizacji polega na cyfrowych rozwiązaniach w codziennej pracy, zabezpieczenia firmy to coś więcej niż alarm przeciwwłamaniowy. Nie czekaj, aż sieć Twojej firmy zostanie zaatakowana – przeprowadź już teraz odpowiednie testy penetracyjne i zabezpiecz się przed niepotrzebnymi stratami!



## Poprzez przeprowadzanie symulacji ataków cybernetycznych na infrastrukturę Klienta:

poznajemy **słabości zabezpieczeń** i skutecznie je wzmacniamy;

identyfikujemy **elementy infrastruktury IT podatne na włamania i dzielimy się najskuteczniejszymi metodami ich zlikwidowania** lub zminimalizowania.

**Bezpieczeństwo infrastruktury IT** stało się kluczowe w funkcjonowaniu firm i wymaga skutecznej identyfikacji słabych punktów, które następnie należy wzmocnić.

# Skuteczne testy bezpieczeństwa

Nasi eksperci wykorzystują technologię open source i komercyjne oprogramowania imitując działania hakerskie w celu znalezienia słabych punktów w sieci klienta.

Testy penetracyjne sieci | Testy penetracyjne aplikacji | Testy penetracyjne sieci bezprzewodowych | Badanie inżynierii społecznej

---

Pentesty - kluczowy krok w kierunku ochrony Twoich danych. Skorzystaj z naszej wiedzy i doświadczenia. Oferujemy precyzyjne raporty i zalecenia, aby poprawić bezpieczeństwo Twojej infrastruktury po przeprowadzonych testach penetracyjnych.

# KROK 3 | Skanowanie podatności

**Skanowanie pod kątem luk w zabezpieczeniach.** Czy zastanawiałeś się kiedykolwiek, jakie luki w zabezpieczeniach mogą się pojawiać w Twoim systemie, oprogramowaniu lub konfiguracji? Jeśli Twoja odpowiedź to „nie” – czas zastanowić się jak się do tego przygotować.

skanowanie luk możliwe jest dzięki **wyspecjalizowanym narzędziom**, które pozwalają zidentyfikować pojawiające się każdego dnia podatności w **systemach, sieciach i aplikacjach** używanych w Twojej firmie;

Smartech IT oferuje usługi **ciągłego monitorowania Twoich systemów** oraz **priorytetyzowania wykrytych luk** w bezpieczeństwie.

Nasz zespół specjalistów bezpieczeństwa cybernetycznego pomoże Ci w terminowym **usuwaniu krytycznych podatności i uniknięciu skutecznych ataków.**

Ciągłe monitorowanie systemów firmy to jeden z **najskuteczniejszych sposobów zapobiegania incydentom oraz włamaniom do infrastruktury IT.** Poprzez skanowanie systemów, oprogramowania oraz konfiguracji pod kątem znanych luk i słabości w zabezpieczeniach jesteśmy w stanie skutecznie przeanalizować w Państwa organizacji potencjalne zagrożenia i im zapobiec.

# KROK 4 | Zarządzanie logami

**Weryfikacja poprawnego gromadzenia i korelacji danych.** W nieuporządkowanej szafie z dokumentami ciężko jest znaleźć konkretny dokument lub zauważyć jego brak. Dokładnie tak samo jest z danymi w Twojej firmie! Poprawne gromadzenie i weryfikacja korelacji danych związanych z dziennikami zdarzeń (log files) jest kluczowa dla zabezpieczenia Twojej firmy.

## Eksperci Smartech-IT mogą kompleksowo przebadać obraz stanu bezpieczeństwa Twojej organizacji poprzez:

- **monitorowanie sieci**;
- **gromadzenie** odpowiednich **plików logów**;
- **ruchu sieciowego i alertów sieciowych;**
- oraz posiadanych przez Ciebie **systemów bezpieczeństwa.**

**W ten sposób umożliwiamy Ci wgląd w realny stan systemu i podejmowanie świadomych decyzji dotyczących Twojej infrastruktury.**

# Dlaczego zarządzanie logami jest istotne?

**Wykrywanie incydentów bezpieczeństwa:** Analiza logów umożliwia identyfikację podejrzanych aktywności, ataków i prób włamań, co pozwala szybko reagować i odpowiednio zabezpieczać systemy.

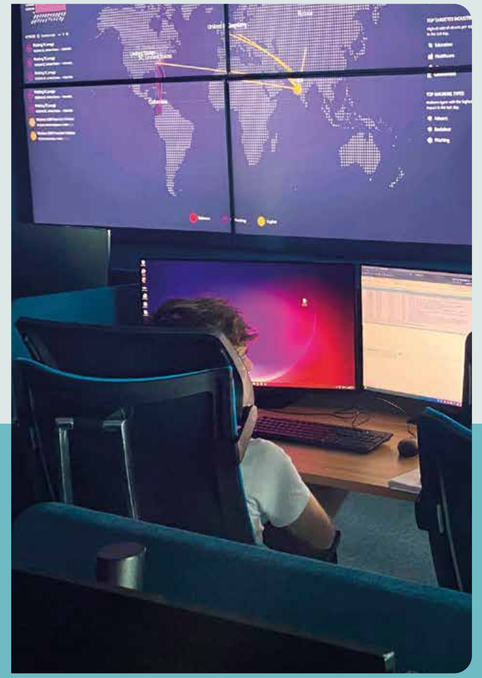
Audyt i zgodność: Zarządzanie logami jest kluczowe dla spełnienia wymagań regulacji i standardów, takich jak RODO, PCI DSS czy SOX. Logi stanowią niezbędny dowód audytu i pomagają udowodnić zgodność z przepisami.

Badanie zdarzeń: Analiza logów pozwala na identyfikację przyczyn awarii systemów, błędów aplikacji czy problemów z wydajnością, co ułatwia proces rozwiązywania problemów.

Zarządzanie logami jest kluczowym elementem skutecznej strategii cyberbezpieczeństwa.

# KROK 5 | Usługi SOC

**naliza w czasie rzeczywistym.** Jeśli Twoja firma posiada monitoring fizyczny w celu bezpieczeństwa pracowników i mienia, dlaczego jeszcze nie skorzystałeś z tego samego rozwiązania dla swojej sieci?



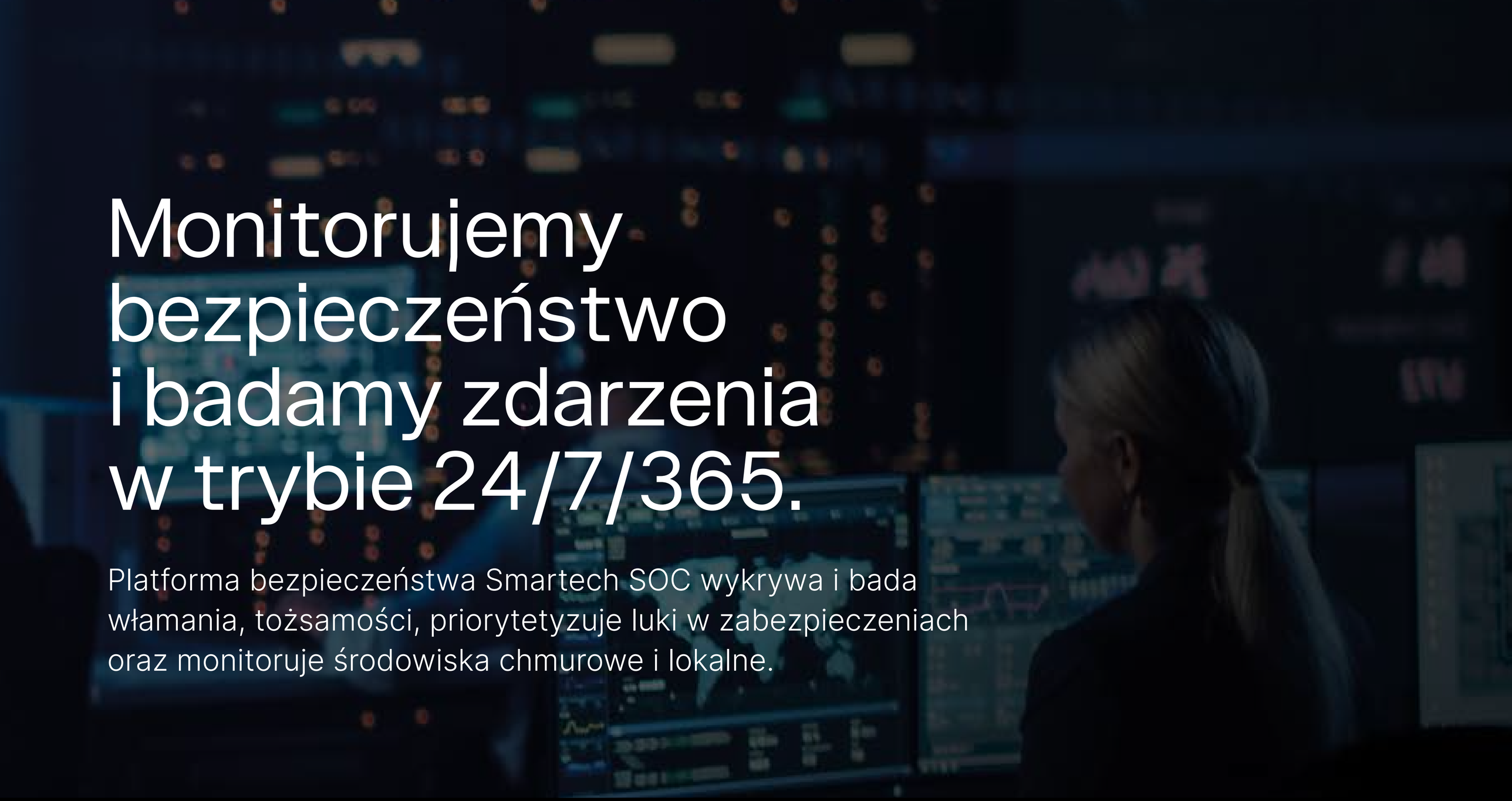
## Smartech IT oferuje:

**analizę w czasie rzeczywistym**

**wykrywanie incydentów bezpieczeństwa** poprzez stałą analizę zebranych i skorelowanych danych.

Dzięki wykorzystaniu zaawansowanej analityki oraz informacji o zagrożeniach, jesteśmy w stanie dla naszych Klientów wykrywać i ustalać priorytety incydentów w oparciu o ich wagi i potencjalny wpływ na działalność organizacji.

Nasza usługa SOC (Centrum Operacji Bezpieczeństwa) oferuje ciągły nadzór, wykrywanie incydentów oraz skuteczną reakcję na zagrożenia, zapewniając wysoki poziom ochrony dla Twojej organizacji.



# Monitorujemy bezpieczeństwo i badamy zdarzenia w trybie 24/7/365.

Platforma bezpieczeństwa Smartech SOC wykrywa i bada włamania, tożsamości, priorytetyzuje luki w zabezpieczeniach oraz monitoruje środowiska chmurowe i lokalne.

# Raportowanie

## Raportowanie i zalecenia po każdym kroku

Klient otrzyma raporty zawierające szczegółowe ustalenia, w zakresie zidentyfikowanych słabych punktów, zagrożeń w posiadanej infrastrukturze przetwarzania danych oraz kluczowe obszary Klienta wymagające poprawy.

Do raportów dołączone zostaną zalecenia, które wskażą zarówno działania możliwe do realizacji od zaraz lub będą do wykorzystania w budżetowaniu środków na kolejne lata. Raporty i zalecenia będą również stanowiły materiał wejściowy do planowania strategii podnoszenia poziomu bezpieczeństwa w organizacji.

Dobrze wiemy, że dla wielu naszych Klientów nasza praca i jej wyniki mogą być niejasne lub czasem brzmieć jak techniczny żargon. Dlatego każda nasza usługa obejmuje dokładny, jasny raport, w którym otrzymasz zaawansowane grafy z przystępnie napisanymi wyjaśnieniami.

W prosty dla Państwa sposób podzielimy się wynikami naszych analiz i zaleceniami, których wprowadzenie podniesie poziom zabezpieczeń w Państwa organizacji.

Smartech IT Sp. z o.o.,
ul. Irysowa 1 (Business Point Bielany)
55-040 Bielany Wrocławskie

biuro@smartech-it.eu
+48 71 727 71 00

www.smartech-it.eu