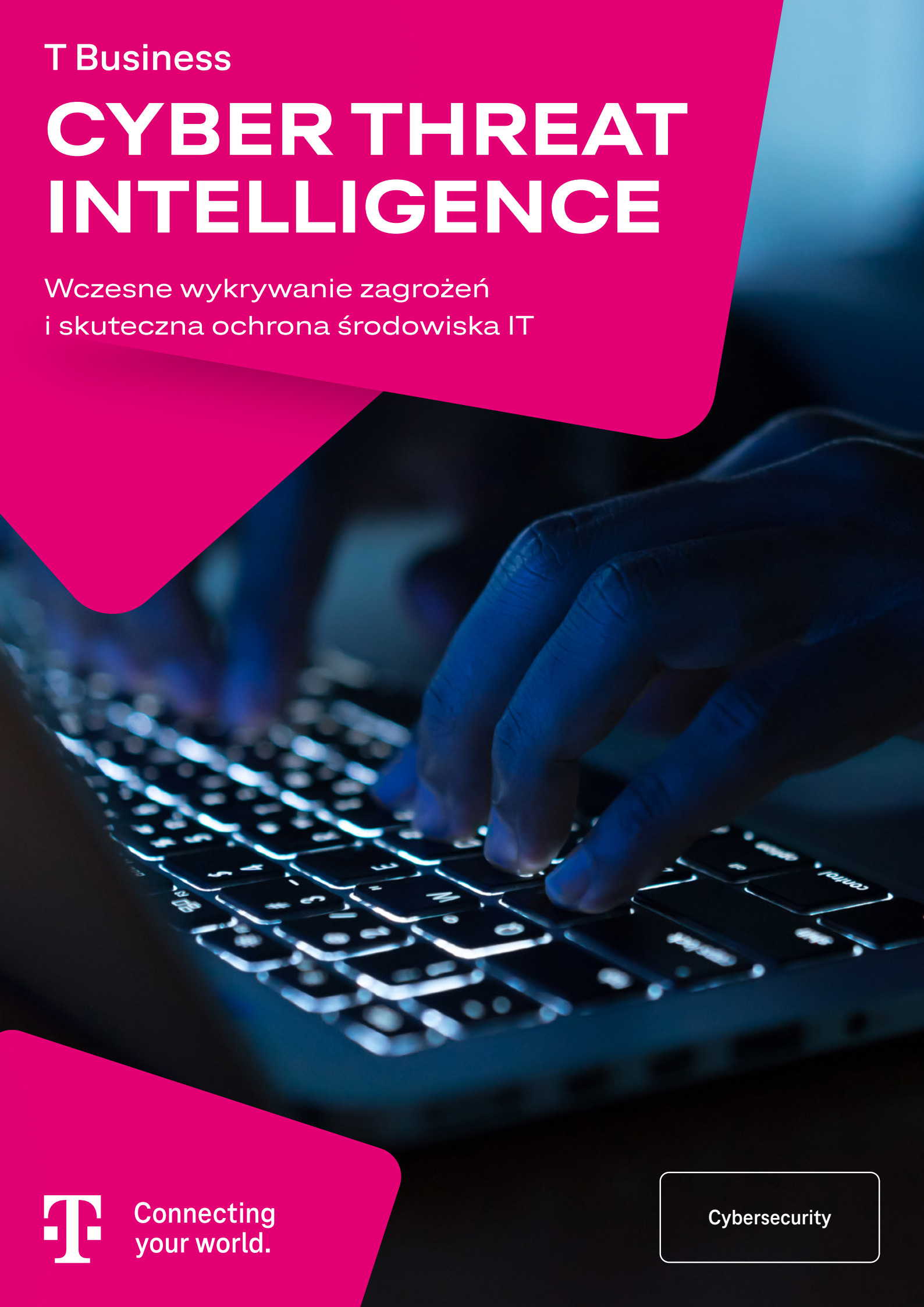
T Business

CYBER THREAT INTELLIGENCE

Wczesne wykrywanie zagrożeń
i skuteczna ochrona środowiska IT



Connecting your world.

Cybersecurity

Opis rozwiązania

Cyber Threat Intelligence (CTI) to usługa przetwarzająca wiedzę o zagrożeniach poprzez analizę informacji o kampaniach ataków, podatnościach i taktykach cyberprzestępców. Umożliwia wczesne rozpoznanie ryzyka oraz ocenę poziomu ekspozycji na zagrożenia, wspierając bardziej świadome i szybsze podejmowanie decyzji w obszarze bezpieczeństwa.

CTI pozwala:

proaktywnie wykrywać zagrożenia,

zrozumieć motywacje, taktyki i działania cyberprzestępców,

redukować ryzyko finansowe, operacyjne i reputacyjne.

Korzyści

- **Widoczność organizacji w sieci**

  Identyfikacja publicznie widocznych zasobów oraz monitorowanie ich ekspozycji i podatności.

- **Wykrywanie wycieków danych**

  Identyfikacja wycieków danych i wzmianek o organizacji w źródłach dark/deep web.

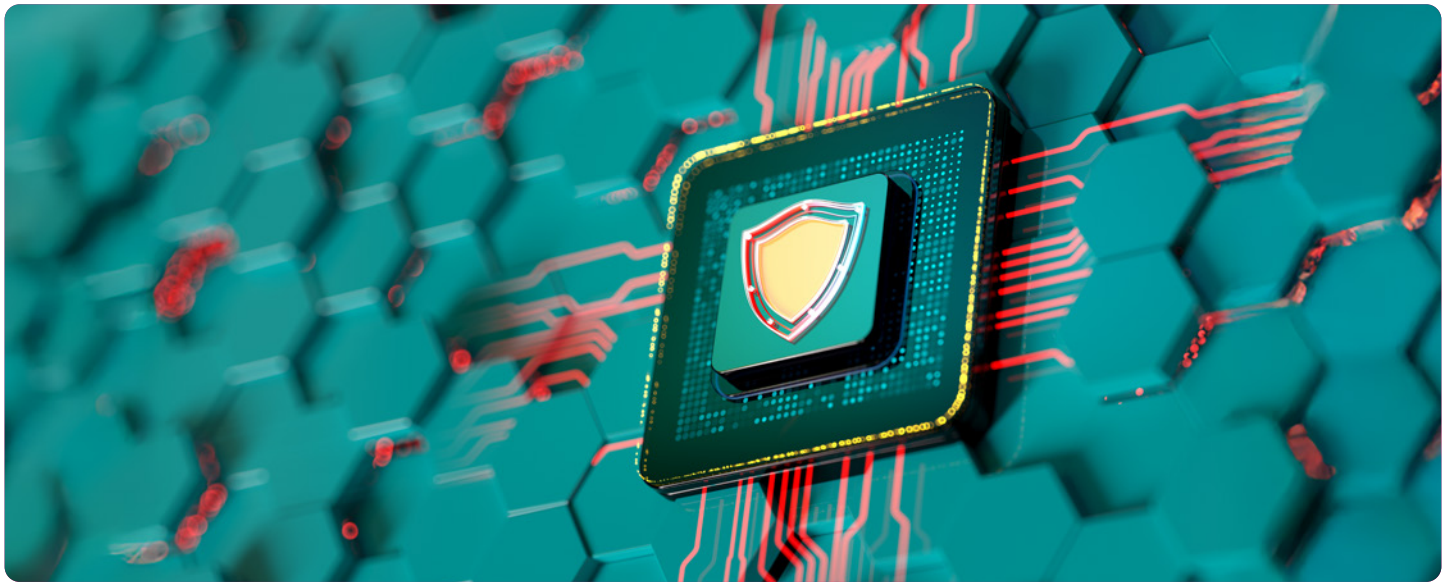
- **Ochrona marki w sieci**

  Wykrywanie domen, aplikacji i kont podszywających się pod organizację.

- **Wgląd w zagrożenia w ekosystemie**

  Analiza kampanii, trendów oraz ryzyka związanego z dostawcami i partnerami.

Cyber Threat Intelligence to przetworzona wiedza, która wspiera wcześniejsze rozpoznanie ryzyka i lepsze decyzje dotyczące bezpieczeństwa.



Jak Cyber Threat Intelligence wzmacnia ochronę organizacji?

Widoczność ryzyka

Lepsza identyfikacja ekspozycji i zależności zwiększających podatność organizacji na atak.

Priorytetyzacja zagrożeń

Koncentracja na zagrożeniach realnie wpływających na organizację i jej otoczenie.

Wcześniejsze wykrywanie nadużyć i wycieków

Szybsze wykrywanie phishingu, podszyć oraz ujawnionych danych.

Zarządzanie ryzykiem w łańcuchu dostaw

Lepsza identyfikacja ryzyk wynikających ze współpracy z dostawcami i partnerami.

Cyber Threat Intelligence wspiera więc bardziej świadome i proaktywne zarządzanie ryzykiem.

Jakie sygnały ostrzegawcze usługa CTI wykrywa z wyprzedzeniem?

Wzmianki o organizacji w podejrzanych źródłach

Informacje o firmie pojawiające się w dark/deep web, na forach, w komunikatorach lub innych kanałach wykorzystywanych przez cyberprzestępców.

Ujawnione dane logowania i wycieki danych

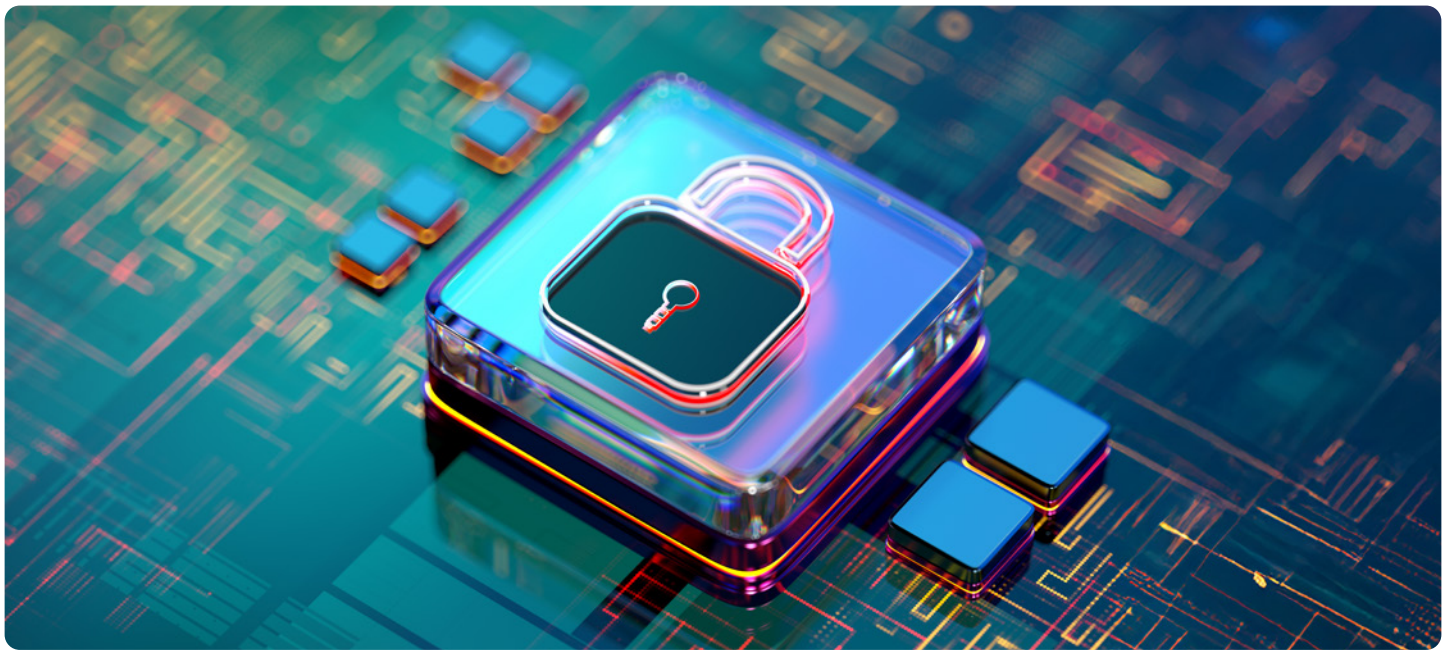
Dane pracowników, klientów lub partnerów, które mogą zostać wykorzystane do przejęcia dostępu, phishingu lub dalszej eskalacji ataku.

Podszywające się domeny, profile i aplikacje

Sygnały wskazujące na wykorzystanie marki organizacji do oszustw, phishingu lub nadużyć wobec klientów i użytkowników.

Ryzyka w otoczeniu organizacji

Zagrożenia po stronie dostawców, partnerów lub w sektorze, które mogą wpływać na działalność, reputację i bezpieczeństwo organizacji.



Przykładowe wykorzystanie Cyber Threat Intelligence

Łańcuch dostaw/transport i logistyka

Cyber Threat Intelligence wspiera organizacje zależne od **dostawców i partnerów biznesowych** we **wcześniejszym rozpoznaniu ryzyk** pojawiających się poza **własną infrastrukturą**. **Usługa pomaga monitorować wzmianki, wycieki danych i sygnały zagrożeń** dotyczące organizacji oraz jej otoczenia biznesowego, wspierając ocenę ryzyka w łańcuchu dostaw i szybsze podejmowanie decyzji ochronnych.

Sektor regulowany/finanse

Cyber Threat Intelligence wspiera organizacje narażone na **phishing**, **podszywanie się pod markę**, **wycieki danych** i **kampanie wymierzone w klientów** lub **usługi cyfrowe**. Usługa pomaga wcześniej wykrywać sygnały zagrożeń, skuteczniej chronić markę oraz szybciej oceniać ryzyko o znaczeniu operacyjnym, reputacyjnym i regulacyjnym.

Cyber Threat Intelligence daje organizacji wcześniejszą wiedzę o zagrożeniach, które mogą przełożyć się na działalność, reputację i bezpieczeństwo klientów.

Dlaczego T-Mobile?

Dostęp do zaawansowanych źródeł danych o zagrożeniach, w tym informacji z dark web i źródeł niedostępnych w standardowych narzędziach.

Skalowalny model współpracy – od podstawowego monitoringu zagrożeń po szersze wsparcie w analizie ryzyka i obsłudze incydentów.

Szerokie portfolio cyberbezpieczeństwa – możliwość włączenia usługi w kompleksowym podejściu do ochrony organizacji i jej środowiska.

Dopasowanie do branży i profilu ryzyka – personalizacja alertów, raportów i zakresu usługi do specyfiki organizacji.

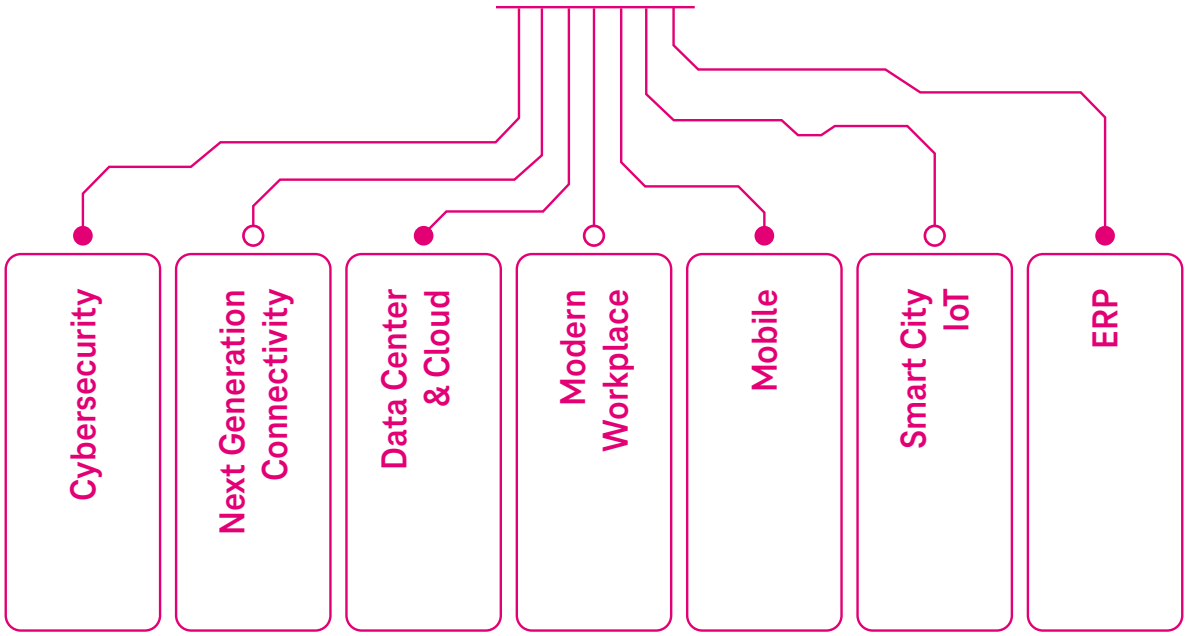
Pakiety i modele współpracy

Bronze	Silver	Gold	Indywidualny
Podstawowy zakres obejmuje monitoring dark webu i identyfikację sygnałów zagrożeń oraz koordynację obsługi incydentów.	Obejmuje zakres Bronze, rozszerzony o widoczność ekspozycji organizacji w Internecie oraz analizę publicznie dostępnych zasobów.	Rozszerzony, kompleksowy zakres Cyber Threat Intelligence obejmuje pogłębioną analizę ryzyka, kampanii zagrożeń, ochronę marki i wsparcie działań bezpieczeństwa.	Zakres usługi dobierany zgodnie z wymaganiami organizacji, profilem ryzyka i oczekiwanym modelem współpracy.

Zakres poszczególnych wariantów może być dopasowany do skali organizacji, jej ekspozycji na ryzyko oraz oczekiwanego poziomu wsparcia.

BUSINESS

KOMPLEKSOWE USŁUGI DLA DUŻYCH I ŚREDNICH FIRM



T-Mobile Polska S.A.
ul. Marynarska 12
02–674 Warszawa

Więcej informacji o usługach:
www.biznes.t-mobile.pl

BE363-003968-00