Cybersecurity

T Business

CYBEROCHRONA DLA FIRM

Connecting your world.

T Business

NAJWYŻSZY POZIOM OCHRONY PRZED CYBERZAGROŻENIAMI

Skala cyberzagrożeń stale rośnie. Wraz z dynamicznym rozwojem technologii i cyfryzacją zwiększa się podatność systemów, powierzchnia ataków oraz ilość przetwarzanych danych. Ataki są coraz liczniejsze i bardziej zaawansowane – cyberprzestępcy wykorzystują nowe techniki, w tym AI, do przełamywania zabezpieczeń i wyłudzania danych.

W tych warunkach cyberochrona staje się niezbędna dla każdej organizacji, niezależnie od jej wielkości i branży. Nowe regulacje, takie jak NIS 2, RODO czy DORA, wymuszają inwestycje w nowoczesne rozwiązania, jednak nawet najlepsze narzędzia nie zapewnią pełnej ochrony bez odpowiedniego podejścia na etapie projektowania, wdrożenia, zarządzania i utrzymania systemów. Kluczowe jest także budowanie świadomości i kompetencji zespołów, ponieważ skuteczna ochrona to proces ciągły, wymagający zaangażowania na każdym poziomie organizacji.

Dlaczego warto współpracować z T-Mobile?

Dostarczamy **kompleksowe rozwiązania**: jesteśmy dostawcą wszystkich niezbędnych komponentów zarówno w warstwie usługowej, sprzętowej, oprogramowania, jak i sieciowej.

Mamy wiele lat doświadczenia w zakresie bezpieczeństwa IT, a nasze wysokie kompetencje potwierdza +30 certyfikatów, m.in.: CPEH, CISSP, CISM, CISA, CompTIA Security+, CompTIA CySA+, OSWP, OSDA, OSCP, SSCP, CEH, CCSE.

Nasze usługi świadczymy w oparciu o uznane na rynku technologie wiodących producentów, takich jak Splunk, QRadar, Fortinet, Palo Alto Networks, Arbor Networks, Radware, Cisco, Qualys, CrowdStrike.

Dysponujemy specjalistycznym zapleczem technologicznym, w tym unikalnym laboratorium do badania podatności urządzeń Internetu Rzeczy.

Nasze Security Operations Center działa 24 godziny, 7 dni w tygodniu, pracuje dla nas ponad **20 inżynierów** bezpieczeństwa w **3 liniach** wsparcia technicznego.

W razie potrzeby **dysponujemy eksperckim wsparciem Grupy Deutsche Telecom.**

KOMPLEKSOWE PORTFOLIO
USŁUG CYBERBEZPIECZEŃSTWA

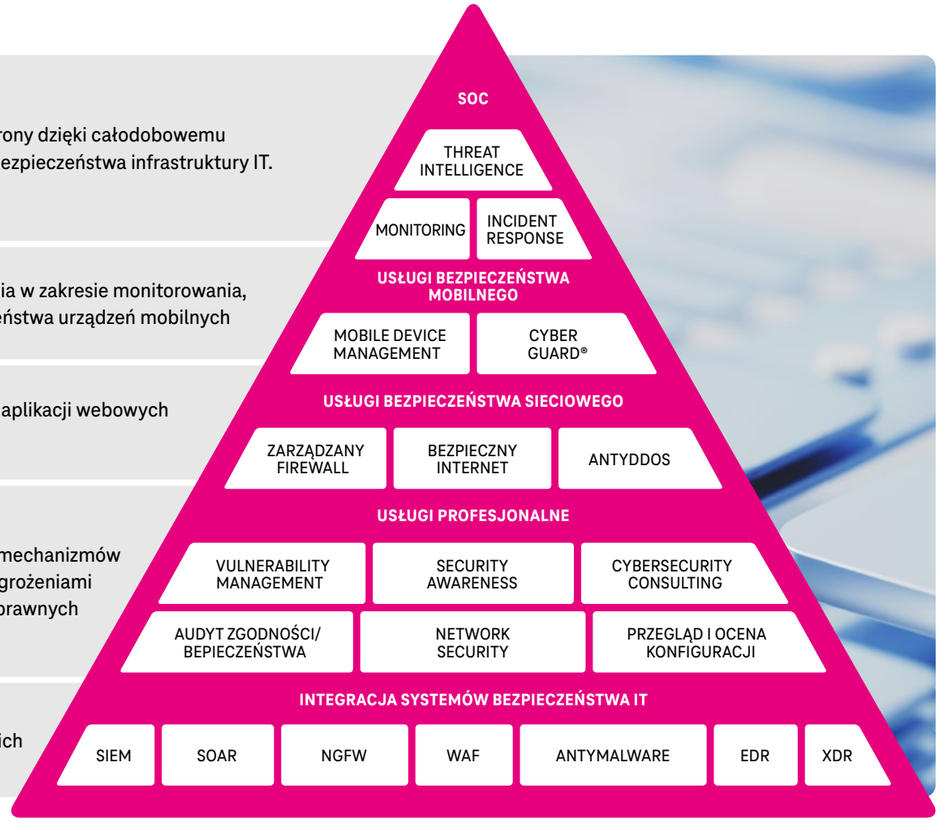
Najwyższy poziom ochrony dzięki całodobowemu monitorowaniu stanu bezpieczeństwa infrastruktury IT.

Innowacyjne rozwiązania w zakresie monitorowania, zarządzania i bezpieczeństwa urządzeń mobilnych

Kompleksowa ochrona aplikacji webowych i sieci komputerowych

Wsparcie w tworzeniu mechanizmów ochrony przed cyberzagrożeniami i spełnianiu wymagań prawnych

Szerokie portfolio rozwiązań integratorskich z obszaru IT Security



SOC – Security Operations Center
Zarządzanie incydentami i bezpieczeństwem IT

Security Operations Center (SOC) to usługa monitorowania i analizy zdarzeń bezpieczeństwa IT w celu wykrywania incydentów związanych z cyberbezpieczeństwem i zapobiegania im w przyszłości. Wykorzystuje najnowsze dostępne rozwiązania technologiczne oraz właściwie określone procesy. Wykwalifikowany zespół, pracujący w trybie 24/7/365, stale monitoruje infrastrukturę IT firmy i na bieżąco rozpoznaje incydenty spośród alertów bezpieczeństwa. Usługa dostarcza niezbędnej wiedzy na temat stanu bezpieczeństwa IT w firmie oraz umożliwia chronienie jej przed cyberzagrożeniami.

W 2024 r. aż **83% polskich firm** doświadczyło przynajmniej jednej próby cyberataku. To **o 43% więcej** niż w 2022 r.

Źródło: KPMG

Usługa wspiera osiągnięcie zgodności z Dyrektywą NIS 2 w zakresie zapobiegania, wykrywania i reagowania na incydenty.

Na usługę SOC składają się:

Monitorowanie i badanie zdarzeń z zakresu bezpieczeństwa 24/7/365 według ustalonych scenariuszy bezpieczeństwa, analiza alertów, identyfikacja incydentów zgodnie z określonym SLA i raporty.

Reakcja na incydent, przedstawienie zaleceń mitygacji, zmierzających do ograniczenia lub eliminacji zagrożeń, prowadzenie działań w celu rozwiązania incydentu zgodnie z określonym SLA.

Threat Intelligence – cykliczne dostarczanie informacji o możliwych nowych zagrożeniach i atakach, sposobach postępowania z nimi i sugerowanych rozwiązaniach zabezpieczających.

SOC Lite
Automatyczna identyfikacja i klasyfikacja zagrożeń

SOC Lite to usługa automatycznego monitorowania i analizy zdarzeń z wielu źródeł w celu wykrywania zagrożeń i incydentów, przy wykorzystaniu systemu i właściwie określonych procesów oraz procedur.

Usługa SOC Lite działa w 5 precyzyjnych krokach:

Wykrycie zagrożenia – identyfikacja potencjalnych zagrożeń w sieci.

Analiza zdarzenia – automatyczna analiza incydentów i danych systemowych.

NOWOŚĆ!

Generowanie alarmu – powiadomienie o zagrożeniach zgodnie z regułami korelacyjnymi.

Klasyfikacja – priorytetyzacja zagrożeń według poziomu krytyczności i raportowanie.

Powiadomienie – informacja e-mail o wykrytym incydencie.

Zarządzany Firewall
Kompleksowa ochrona sieci

Zarządzany Firewall dostarcza wiele mechanizmów do kontroli ruchu sieciowego oraz ochrony użytkowników przed zagrożeniami z Internetu. Usługa obejmuje uruchomienie firewalla nowej generacji, konfigurację oraz zaimplementowanie polityk bezpieczeństwa w celu ochrony sieci. T-Mobile gwarantuje również utrzymanie firewalla, administrację w trybie 24/7, wsparcie techniczne oraz zarządzanie, z uwzględnieniem aktualizacji bezpieczeństwa, konfiguracji nowych polityk, tworzenia cyklicznych raportów. Usługa ta dostępna jest na łączu internetowym od dowolnego operatora.

W 2024 r. CERT Polska odnotował ponad **600 tys. zgłoszeń potencjalnych incydentów**, co oznacza wzrost o 62% w stosunku do roku poprzedniego.

Usługa jest przeznaczona dla wszystkich firm, zwłaszcza tych o rozproszonej strukturze oraz klientów T-Mobile korzystających z usługi dostępu do Internetu czy Sieci Korporacyjnych.

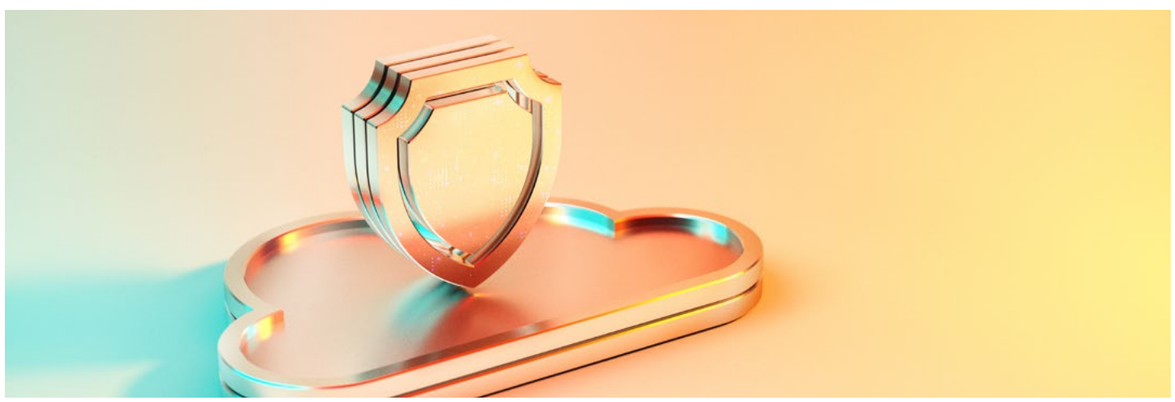
AntyDDoS
Ochrona przed atakami DDoS

Usługa AntyDDoS wyposażona w mechanizmy detekcji, wielopoziomowe zabezpieczenia oraz wysoce wydajny system filtracji pozwala zabezpieczyć klienta nawet przed największymi atakami wolumetrycznymi oraz aplikacyjnymi. Dzięki ww. ochronie możemy skutecznie rozróżnić ruch sztuczny od prawidłowego.

Liczba ataków DDoS na warstwę aplikacji (web DDoS) wzrosła w 2024 r. o **550%** w porównaniu z rokiem poprzednim.

Źródło: Radware

Usługa jest przeznaczona dla wszystkich klientów T-Mobile, korzystających z usługi dostępu do Internetu.



Cloud Application Protection
Inteligentna ochronay aplikacji webowych, stron www oraz API

Cloud Application Protection to kompleksowa usługa ochrony stron www, aplikacji webowych oraz API, świadczona w chmurze, wykorzystująca mechanizmy uczenia maszynowego oraz sztucznej inteligencji. Swoim zakresem obejmuje m.in.: web application firewall, ochronę przed botami, ochronę przed atakami aplikacyjnymi, atakami DDoS oraz ochronę API. Usługa dostępna jest w trzech pakietach, które umożliwiają elastyczne dopasowanie zakresu ochrony do indywidualnych potrzeb firmy.

Ataki typu DDoS w 2024 r. są najczęściej zgłaszanym zagrożeniem w Unii Europejskiej i stanowią aż **33% wszystkich incydentów**.

Źródło: Threat Landscape 2024

Usługa przeznaczona dla firm , która chcą chronić swoje aplikacje internetowe oraz API przed zaawansowanymi zagrożeniami bez konieczności utrzymywania własnej infrastruktury bezpieczeństwa.

MDM (Mobile Device Management)
Zabezpieczenie urządzeń mobilnych

MDM T-Mobile jest rozwiązaniem pozwalającym na zarządzanie urządzeniami mobilnymi przez cały cykl ich życia. Usługa ta daje do dyspozycji narzędzia pozwalające na konfigurację, zarządzanie oraz zabezpieczanie urządzeń korzystających z systemów operacyjnych iOS, Android, macOS i Windows w sposób zdalny. Z wykorzystaniem MDM T-Mobile administratorzy będą mogli między innymi przeprowadzać zdalne instalacje i aktualizacje aplikacji, cykliczny backup danych oraz śledzić lokalizację urządzenia.

Usługa ta przeznaczona jest dla firm szukających rozwiązania, które umożliwia pełną kontrolę nad flotą urządzeń mobilnych.

Cyber Guard®

Cyber Guard® jest autorskim rozwiązaniem T-Mobile Polska, chroniącym przed cyberzagrożeniami na możliwie najwcześniejszym etapie ich wykrycia. Narzędzie to analizuje automatycznie, za pomocą stworzonych przez T-Mobile algorytmów, ruch sieciowy pod kątem cyberzagrożeń. Dzięki wykorzystaniu elementów Big Data analizuje miliardy sesji internetowych każdego dnia. Rozwiązanie to jest w stanie precyzyjnie zidentyfikować zainfekowane złośliwym oprogramowaniem wszelkiego rodzaju urządzenia komunikujące się w oparciu o protokół TCP/IP. Cyber Guard® analizuje cały ruch w sieci operatora w celu wykrywania wszelkich zagrożeń w cyberprzestrzeni, a także automatycznie blokuje złośliwe sesje.

CYBER GUARD®

Rozwiązanie Cyber Guard® tylko w okresie od listopada 2024 r. do lutego 2025 r. zablokowało ponad **393 tys. zagrożeń**.

Usługa ta przeznaczona jest dla przedsiębiorstw szukających skutecznego narzędzia do monitorowania i zabezpieczania firmowych urządzeń mobilnych.

Cyber Know
Symulowane ataki i szkolenia Security Awareness

Cyber Know to nowoczesne narzędzie wspierające budowę kultury cyberbezpieczeństwa w organizacjach. Umożliwia realizację realistycznych symulacji ataków phishingowych i smishingowych, które pozwalają diagnozować poziom odporności pracowników na zagrożenia oraz identyfikować obszary wymagające edukacji.

Analiza wyników kampanii symulacyjnych dostarcza cennych informacji na temat luk w świadomości użytkowników i stanowi podstawę do skutecznego kształtowania nawyków związanych z cyberhigieną. Rozwiązanie wspiera systematyczne podnoszenie poziomu tzw. Security Awareness, stanowiącego dziś kluczowy element strategii bezpieczeństwa informacji w każdej organizacji.

72% pracowników przyznaje, że **doświadczyło incydentu cyberbezpieczeństwa** na służbowym sprzęcie, a tylko **26%** pracowników **uczestniczyło w szkoleniach z zakresu cyberbezpieczeństwa** więcej niż jeden raz.

Źródło: Cyberportret polskiego biznesu 2024

Usługa wspiera zgodność z Dyrektywą NIS 2 w zakresie podstawowych praktyk cyberhigieny oraz szkoleń z cyberbezpieczeństwa.

Bezpieczny Internet
Ochrona punktu styku z siecią Internet

Pakiet Bezpieczny Internet gwarantuje kompleksową ochronę punktu styku z Internetem, która opiera się na mechanizmach do kontroli ruchu sieciowego. Usługa Bezpieczny Internet zabezpiecza użytkowników przed zagrożeniami z Internetu, w oparciu o Firewall Nowej Generacji. T-Mobile zapewnia konfigurację poprzez zaimplementowanie polityk bezpieczeństwa, utrzymanie, administrację, wsparcie techniczne 24/7, zarządzanie z uwzględnieniem aktualizacji bazy zagrożeń oraz tworzenie cyklicznych raportów.

Raport ENISA „Threat Landscape 2024” pokazuje, że wśród 11 079 incydentów **ransomware** stanowił **18%**, **malware 9%**, a szkody spowodowane **nieautoryzowanym dostępem** odnotowano w **60%** przypadków naruszeń bezpieczeństwa.

Usługa jest przeznaczona dla wszystkich klientów T-Mobile korzystających z usługi dostępu do Internetu (w tym taryfy LTE/5G).

PROFESJONALNE WSPARCIE
W PROJEKTOWANIU MECHANIZMÓW OCHRONY ORAZ ZAPEWNIANIU ZGODNOŚCI Z PRZEPISAMI

Usługi profesjonalne zapewniają przede wszystkim dostęp do wiedzy i wieloletnich doświadczeń inżynierów ds. bezpieczeństwa IT T-Mobile.

W ramach oferty świadczone są następujące usługi:

Testy penetracyjne infrastruktury, aplikacji i sieci przeprowadzane zgodnie z najlepszymi przyjętymi na rynku praktykami oraz symulowane cyberataki na zlecenie klienta.

Audyty bezpieczeństwa, w tym audyty zgodności np. z NIS 2, RODO, PCI DSS, ISO 2701.

Szkolenia podnoszące świadomość w zakresie bezpieczeństwa IT oraz specjalistyczne, przeznaczone dla administratorów i osób zarządzających systemami zabezpieczeń IT.

Doradztwo w zakresie architektury systemów bezpieczeństwa, w tym testy porównawcze różnych technologii i ocena produktów dostawców.

Analiza poincydentalna, analiza malware, badanie śladów, które pozwalają na identyfikowanie złośliwego kodu i zbieranie materiału dowodowego zgodnie z przepisami prawa.

Testy zabezpieczeń IoT, badanie podatności urządzeń Internetu Rzeczy przeprowadzane w specjalistycznym laboratorium T-Mobile.

Program Zarządzania Podatnościami minimalizuje ryzyka wystąpienia zagrożenia poprzez identyfikację oraz mitygację podatności w infrastrukturze IT klienta.

Usługi profesjonalne to rozwiązania skierowane do firm, które chcą ocenić poziom zabezpieczeń swojej infrastruktury IT i poznać skuteczne metody budowania mechanizmów ochrony przed zagrożeniami.

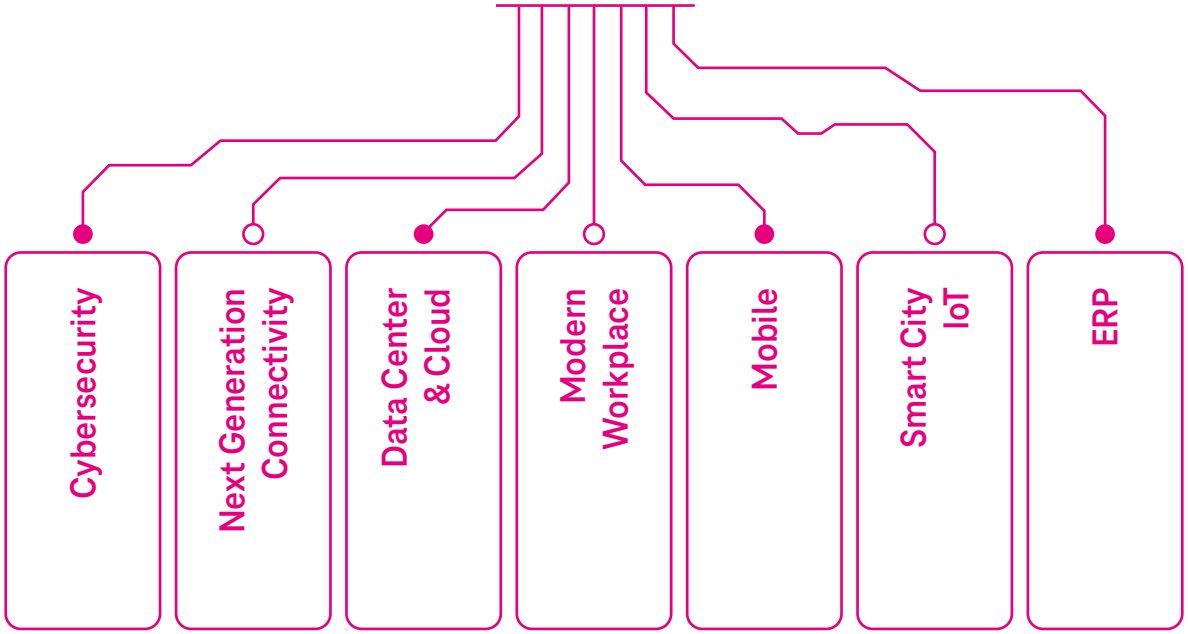
To realne wsparcie np. w spełnieniu wymagań Dyrektywy NIS 2 – od identyfikacji luk w systemach po praktyczne wskazówki dotyczące wdrażania odpowiednich zabezpieczeń.

ROZWIĄZANIA T BUSINESS
WSPIERAJĄCE ZGODNOŚĆ Z NIS 2

WYMAGANIA NIS 2	DEDYKOWANE ROZWIĄZANIE	DLACZEGO T BUSINESS?
Analiza ryzyka oraz polityka bezpieczeństwa systemów informatycznych	• Usługi profesjonalne: doradztwo	• Zarządzanie Programem Bezpieczeństwa . • Analiza stanu bezpieczeństwa, przygotowanie planu i schematu działania • Ustalenie najlepszych praktyk w zakresie zasad i procedur, które zgodne są z ramami cyberbezpieczeństwa NIS 2 i innymi obowiązującymi regulacjami branżowymi
Zapobieganie incydentom, wykrywanie ich i reagowanie na nie	• **Security Operations Center (SOC)** • **XDR** • **Cyber Guard®** • **Zarządzany Firewall** • **AntyDDoS** • Usługi profesjonalne: doradztwo	• Usługi wspierane analitykami SOC oraz analitykami wykrywającymi zagrożenia w cyberprzestrzeni • Usługi poprawiające bezpieczeństwo podczas korzystania z Internetu • Planowanie reagowania na incydenty związane z cyberbezpieczeństwem
Zapewnienie ciągłości działania i zarządzanie kryzysowe	• **MetroCluster** • **Disaster Recovery as a Service** • **Backup** • **AntyDDoS**	• Usługi zwiększające dostępność zasobów • Eliminowanie przerw wynikających z niedostępności systemów
Zapewnienie bezpieczeństwa w pozyskiwaniu, rozwijaniu oraz utrzymywaniu sieci i systemów informatycznych, zarządzanie podatnościami	• **Program Zarządzania Podatnościami (Vulnerability Management)** • Dostawa i wdrożenie rozwiązań z zakresu automatyzacji testów pozwalających na wykrywanie podatnośc • Dostawa i wdrożenie rozwiązań z zakresu cyberbezpieczeństwa przez wykwalifikowany personel przy zapewnieniu zgodności z normami (ISO itp.)	• Ocena stanu infrastruktury teleinformatycznej • Badanie bezpieczeństwa i zabezpieczeń aplikacji WEB • Analiza nadzoru nad punktem styku z Internetem • Weryfikacja sposobu ochrony systemów pocztowych • Ocena stanu kultury bezpieczeństwa • Wykrywanie podatności
Podstawowe praktyki cyberhigieny i szkolenia z zakresu budowania świadomości bezpieczeństwa	• **Security Awareness: Cyber Know** • **Security Awareness: KnowBe4** • **Mobile Device Management (MDM)**	• Szkolenie podnoszące świadomość bezpieczeństwa pozwala zmniejszyć ryzyko podatności na ataki wykorzystujące socjotechnikę • Pomagamy zmieniać zachowania pracowników Celem jest zwiększenie odporności na najnowsze zagrożenia socjotechniczne i taktyki naruszania biznesowej poczty elektronicznej

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

Numer jobu: 14253092