Dbamy o cyberbezpieczeństwo w placówkach medycznych

Skorzystaj ze specjalnej oferty od Orange

Część Orange Polska

INTEGRATED SOLUTIONS

orange™

Co zabezpieczy placówkę przed skutkami cyberataków?

Codziennie pojawiają się nowe rodzaje i metody ataków, które mogą spowodować ograniczenie funkcjonowania organizacji. Placówki medyczne także są na nie narażone. Zablokowanie dostępu do systemu informatycznego szpitala i niemożność przyjmowania pacjentów bądź przeprowadzenia operacji, utrata danych podopiecznych placówki – to może być efekt działania cyberprzestępców.

Zabezpieczenie placówki przed skutkami cyberataków przez:

- weryfikację posiadanych zabezpieczeń,
- tworzenie kopii zapasowych i bezpieczne ich utrzymywanie,
- programy antywirusowe,
- rozwiązania zabezpieczające sieć,
- systemy identyfikujące zagrożenia,
- szkolenia z zakresu budowania świadomości zagrożeń oraz kompetencji cyfrowych pracowników.

Eksperci Orange przygotowali ofertę dla szpitali, aby chronić je przed:

- nieuprawnionym dostępem do systemów informatycznych,
- wyciekiem danych wrażliwych pacjentów oraz personelu,
- zablokowaniem systemów informatycznych,
- upublicznieniem lub wykasowaniem kartotek pacjentów,
- zaszyfrowaniem danych,
- zablokowaniem dostępu do strony WWW.

Co oferujemy w zakresie bezpieczeństwa?

Kompleksowe rozwiązania dla placówek medycznych od jednego dostawcy

1. Audyt – przegląd bezpieczeństwa placówki medycznej

Przegląd i ocena procesów bezpieczeństwa informacji pod kątem ich zgodności z normami i przepisami prawa. Doradztwo oraz wsparcie przy zabezpieczaniu przetwarzania informacji.

Gwarantujemy zgodność z przepisami i normami ISO 27001, 27799:2016-10, ISO 22301, ustawą o krajowym systemie cyberbezpieczeństwa, RODO.

2. Cyber Pakiet

Zestaw profesjonalnych usług, dzięki którym monitorujemy bezpieczeństwo, wykrywamy luki i pomagamy w budowaniu bezpiecznego środowiska informatycznego placówki poprzez:

- skanowanie podatności na cyberataki, w tym kontrolę i ocenę stanu bieżącego konfiguracji infrastruktury,
- ochronę reputacji – monitoring w zakresie nadzoru nad systemami IT, m.in. nad ważnością certyfikatów,
- testy penetracyjne przeprowadzane przez ekspertów z zakresu bezpieczeństwa, którzy sprawdzą bezpieczeństwo najistotniejszych elementów infrastruktury oraz wskazanych webaplikacji,
- budowanie świadomości zagrożeń i szkolenia dla pracowników placówek.

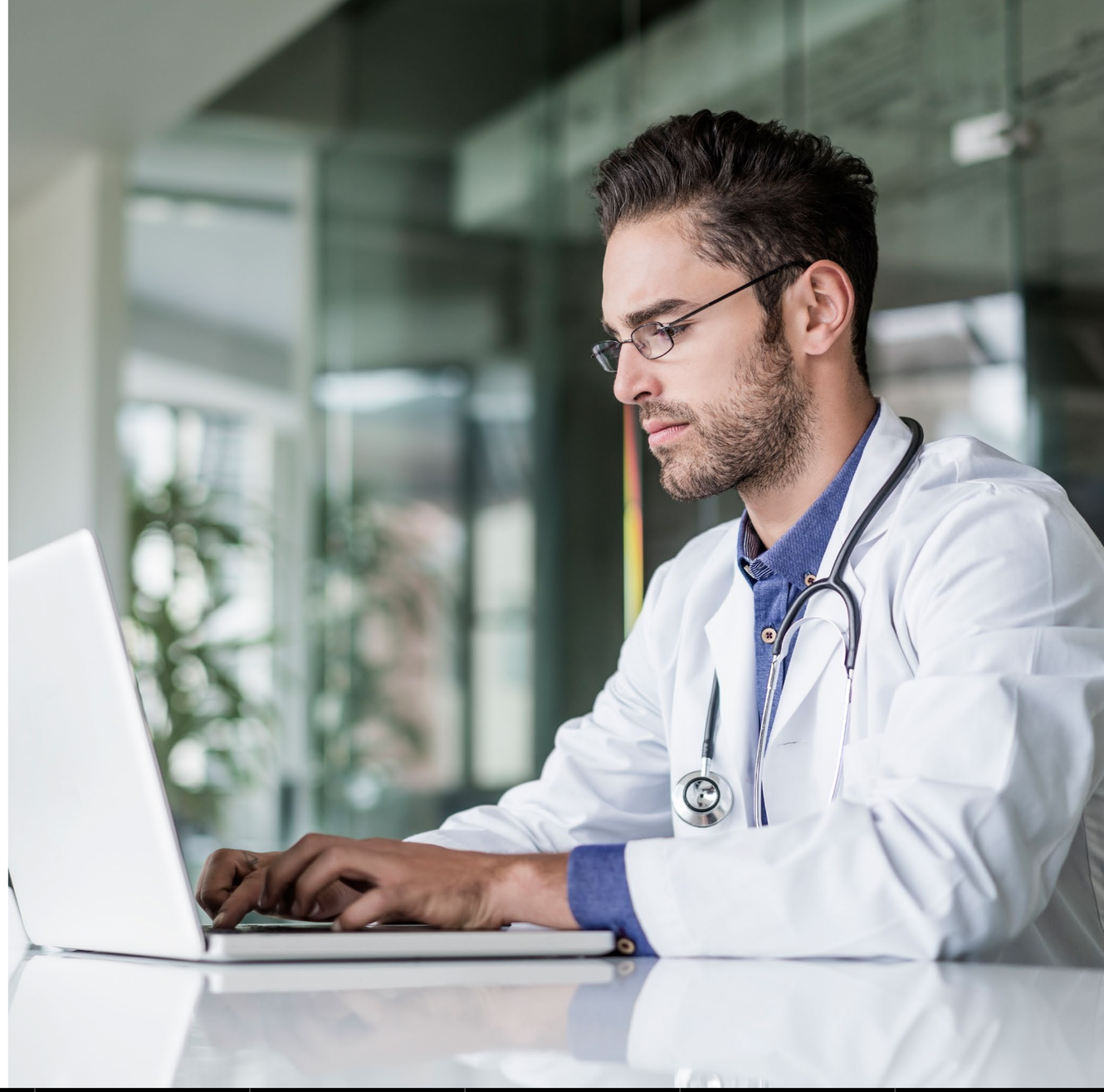
3. SOC LITE

W pełni zautomatyzowana usługa monitorująca, wykrywająca incydenty bezpieczeństwa w sieci i informująca o nich.

Analiza i kontrola bezpieczeństwa

Automatyzacja pracochłonnych działań

Ograniczenie kosztów i czasu wykonywania zadań

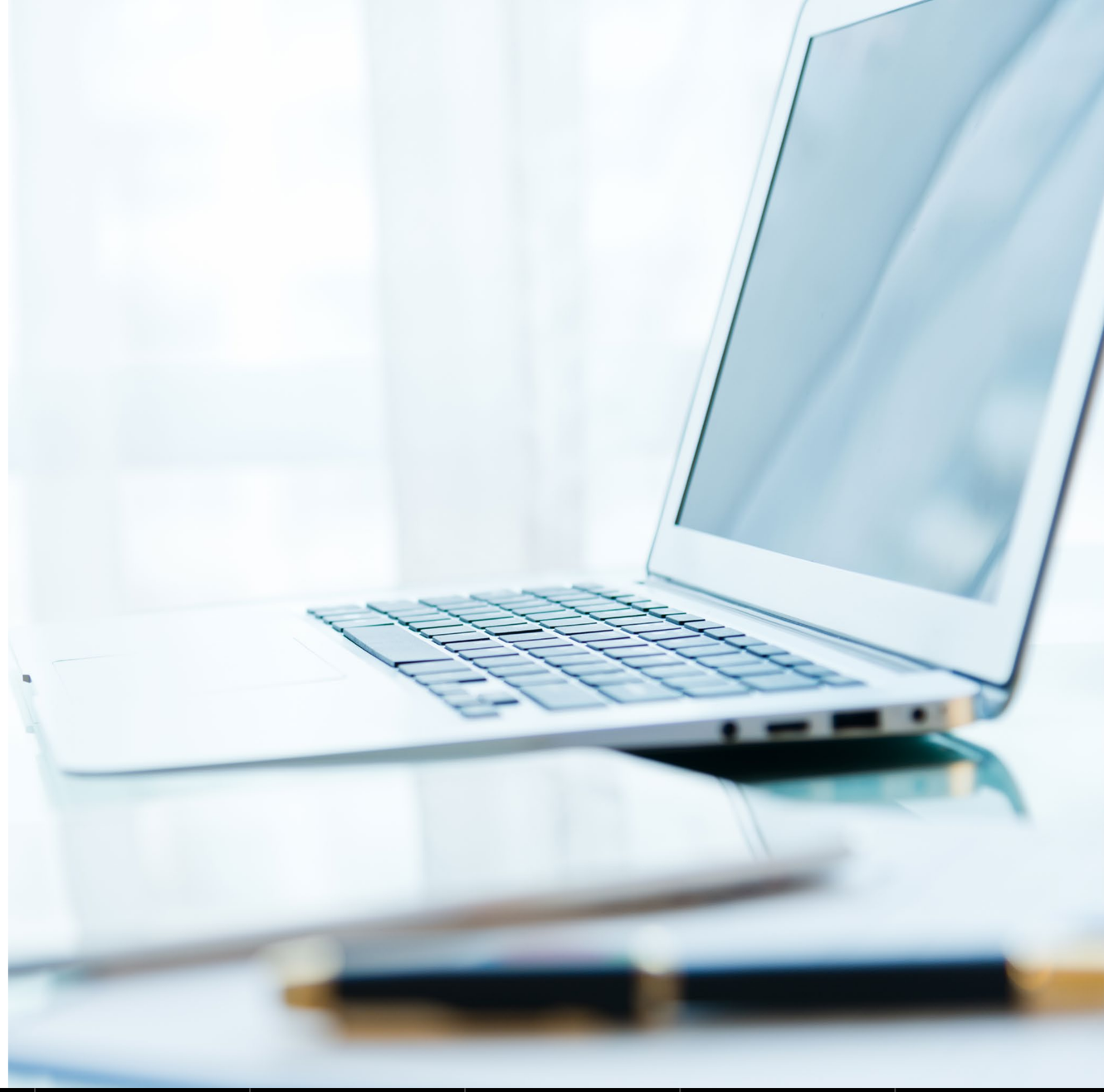


4. Next Generation Firewall

- Monitoruje ruch sieciowy.
- Blokuje:
  - połączenia przychodzące z internetu,
  - niepożądane próby udostępniania danych z komputerów sieci lokalnej do sieci zewnętrznej.
- Umożliwia dokładne filtrowanie dostępu na poziomie sieci lokalnej (LAN), domowej oraz na indywidualnych komputerach.
- Zabezpiecza i skutecznie chroni przed skanowaniem portów oraz próbami zainfekowania komputera, chęcią podsłuchów i wysyłania wiadomości mających na celu przechwycenie i kradzież danych.

Zapewnia:

- firewall,
- IPS,
- antywirus,
- web filtering,
- kontrolę aplikacji,
- Sandbox,
- SD WAN,
- raportowanie.



4a. Next Generation Firewall

Orange Network Security
(urządzenie w sieci Orange)

Zapewnia:

- bezpieczny dostęp do internetu,
- brak inwestycji w sprzęt – infrastruktura w chmurze Orange,
- optymalizację kosztów poprzez kombinację usług internet-VPN-security,
- blokowanie ataków już w sieci Orange, przed dotarciem do sieci placówki,
- scentralizowaną politykę bezpieczeństwa dla wszystkich oddziałów placówki,
- dostęp do portalu wykorzystywanego przez placówkę do zarządzania usługą.

Zarządzany UTM
(urządzenie w sieci klienta)

Zapewnia:

- bezpieczny dostęp do internetu,
- optymalizację kosztów poprzez kombinację usług internet-VPN-security,
- scentralizowaną politykę bezpieczeństwa dla wszystkich oddziałów placówki,
- jednego dostawcę usług internetowych, data i security.

Odsprzedaż urządzeń i licencji

Zapewniamy:

- pomoc, doradztwo oraz dobór najlepszej oferty na rynku w zakresie zakupu,
- dostarczenie urządzenia UTM.

5. Cyber Watch

Usługa platformowa chroniąca łącza oraz urządzenia (smartfony, komputery, routery, urządzenia IoT) korzystające z sieci Orange przed połączeniami stanowiącymi zagrożenie.

Zapewnia:

identyfikację zainfekowanych urządzeń korzystających z sieci Orange

blokadę komunikacji ze stronami stanowiącymi zagrożenie dla danej placówki medycznej

codzienny raport o wykrytych próbach połączeń stanowiących zagrożenie (typu malware, ransomware, phishing)

6. Orange Internet Protection

To kompleksowa ochrona przed atakami DDoS (Distributed Denial of Service). Mogą one zakłócić np. działanie strony internetowej szpitala.

Zapewnia:

stały monitoring ruchu sieciowego

wykrycie i blokadę ataku

przekierowanie prawidłowego ruchu do klienta

7. Rozwiązania pakietowe

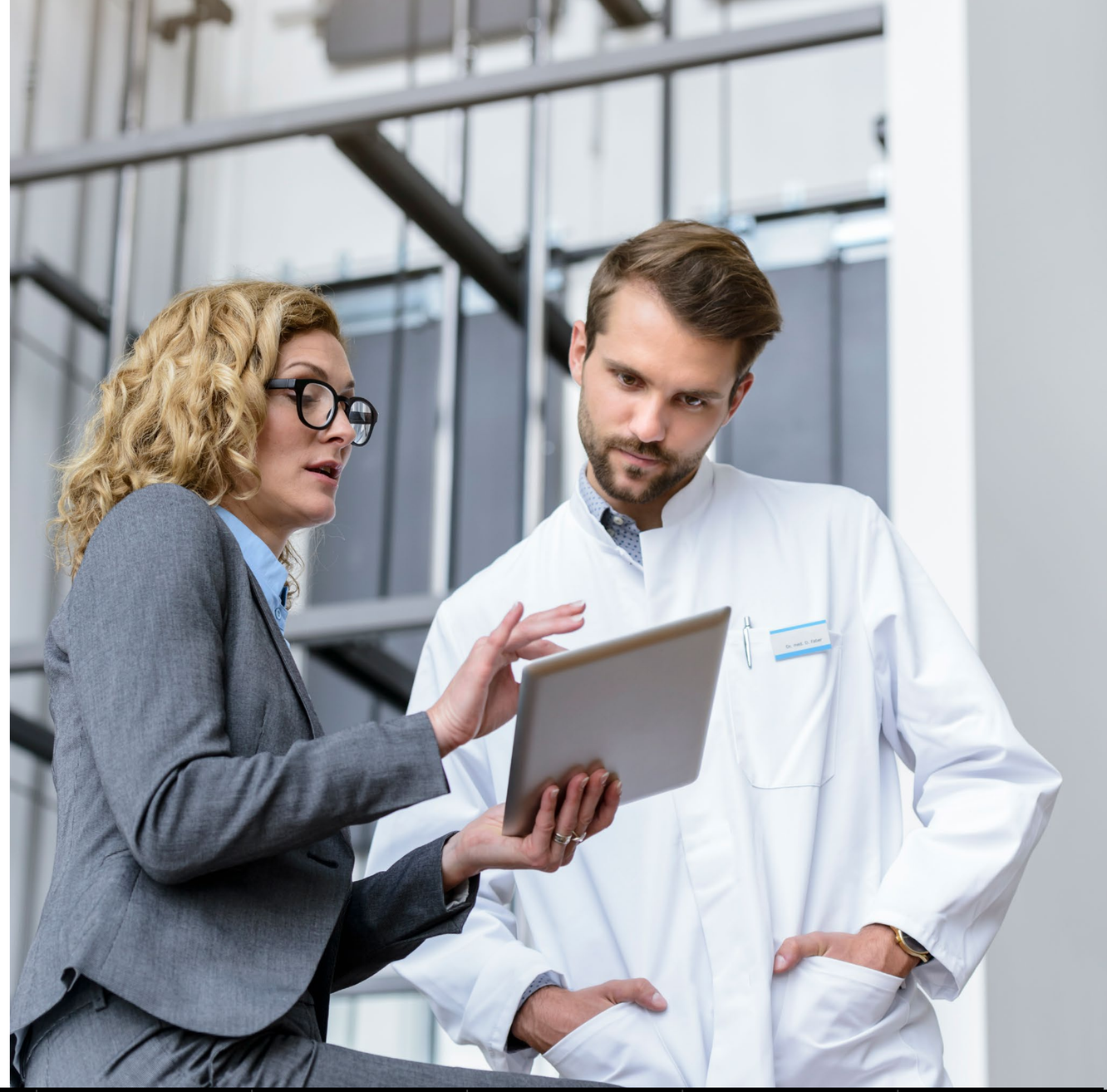
Zestaw Basic

SOC Lite z ONS lub Zarządzanym UTM

Zestaw Premium

SOC Lite z ONS lub Zarządzanym UTM

Cyber Pakiet Minimum



Chcesz dowiedzieć się więcej o naszych rozwiązaniach?

Odwiedź naszą stronę:
orange.pl/duze-firmy/cyberbezpieczenstwo

lub skontaktuj się ze mną